McAfee®

Internet Security Suite 2007

Guia do Usuário

Conteúdo

C A P Í T U L O 1

McAfee Internet Security

O McAfee Internet Security Suite permite que você tenha uma experiência sem preocupações na Internet, protegendo sua identidade e o computador contra ameaças on-line e oferecendo backup automatizado de arquivos importantes. A proteção confiável da McAfee está sempre ativa, sempre atualizada e sempre protegendo na Internet, por isso você pode navegar, fazer compras e transações bancárias, enviar e-mails, participar de bate-papos e fazer download de arquivos com segurança. A McAfee também facilita a exibição do seu status de segurança, a varredura contra spyware e vírus e garante que seus produtos estejam atualizados através do novo McAfee SecurityCenter. Além disso, você receberá a última versão do software e as últimas atualizações da McAfee automaticamente, com sua assinatura.

O Internet Security inclui os seguintes programas:

- SecurityCenter
- Privacy Service
- Shredder
- VirusScan
- Personal Firewall
- SpamKiller
- Backup de dados
- Network Manager
- EasyNetwork (apenas com licença para 3 usuários)
- SiteAdvisor

CAPÍTULO 2

McAfee SecurityCenter

O McAfee SecurityCenter é um ambiente fácil de usar, no qual os usuários da McAfee podem iniciar, gerenciar e configurar suas assinaturas de segurança.

O SecurityCenter também funciona como uma fonte de informações sobre alertas de vírus, produtos, suporte, assinaturas e como acesso com um único clique às ferramentas e às notícias do site da McAfee na Web.

Neste capítulo

Recursos

O McAfee SecurityCenter possui os seguintes novos recursos e benefícios:

Status de proteção reprojetado

Analise facilmente o status da segurança do computador, verifique se há atualizações e corrija potenciais problemas de segurança.

Upgrades e atualizações contínuos

Instalação automática de atualizações diárias. Quando há uma nova versão do software McAfee disponível, você a recebe automaticamente sem custo adicional durante sua assinatura, garantindo que você sempre tenha a proteção mais recente.

Alertas em tempo real

Os alertas de segurança notificam sobre epidemias de vírus emergenciais e ameaças à segurança. Também oferecem opções de resposta para remover, neutralizar ou aprender mais sobre a ameaça.

Proteção conveniente

Diversas opções de renovação ajudam a manter sua proteção McAfee atualizada.

Ferramentas de desempenho

Remova arquivos não utilizados, desfragmente arquivos utilizados e use a restauração do sistema para manter seu computador funcionando com o máximo de desempenho.

Ajuda on-line real

Obtenha suporte de especialistas em segurança de computador da McAfee, via bate-papo na Internet, e-mail e telefone.

Proteção de navegação segura

Quando instalado, o plug-in para navegador do McAfee SiteAdvisor ajuda a proteger contra spyware, spam, vírus e fraudes on-line, classificando sites da Web que você visita ou que aparecem em seus resultados de pesquisa na Web. Você pode exibir classificações de segurança detalhadas para mostrar os resultados dos testes do site em relação a práticas de e-mail, downloads, afiliações on-line e inconvenientes como pop-ups e cookies de rastreamento de terceiros.

CAPÍTULO 3

Usando o SecurityCenter

Você pode executar o SecurityCenter a partir do ícone do McAfee SecurityCenter na área de notificação do Windows na extrema direita da barra de tarefas, ou na área de trabalho do Windows.

Quando o SecurityCenter é aberto, o painel Início exibe o status da segurança do computador e fornece acesso rápido a atualizações, varredura (se o McAfee VirusScan estiver instalado) e outras tarefas comuns:

Cabeçalho

Ajuda

Exibir o arquivo de Ajuda do programa.

Coluna esquerda

Atualizar

Atualize seu produto para se proteger contra as ameaças mais recentes.

Varredura

Se o McAfee VirusScan estiver instalado, você poderá executar uma varredura manual em seu computador.

Tarefas comuns

Execute tarefas comuns, incluindo retornar ao painel Início, exibir eventos recentes, gerenciar a rede do computador (se for um computador com recursos de gerenciamento para esta rede) e manutenção do computador. Se o McAfee Data Backup estiver instalado, você também poderá fazer backup de dados.

Componentes instalados

Veja quais serviços de segurança estão protegendo seu computador.

Painel principal

Status de proteção

Em **Estou protegido?**, consulte o nível geral do status de proteção do computador. Abaixo desta opção, exiba uma análise do status por categoria ou tipo de proteção.

Informações do SecurityCenter

Veja quando ocorreu a última atualização de seu computador, quando ocorreu a última varredura (se o McAfee VirusScan estiver instalado), além da data de expiração da assinatura.

Neste capítulo

Noções básicas sobre os ícones do SecurityCenter

Os ícones do SecurityCenter aparecem na área de notificação do Windows, na extrema direita da barra de tarefas. Use-os para saber se seu computador está totalmente protegido, para exibir o status de uma varredura em andamento (se o McAfee VirusScan estiver instalado), verificar atualizações, exibir eventos recentes, fazer a manutenção do computador e para obter suporte no site da McAfee na Web.

Abra o SecurityCenter e use recursos adicionais

Quando o SecurityCenter está sendo executado, o ícone M do SecurityCenter aparece na área de notificação do Windows, na extrema direita da barra de tarefas.

Para abrir o SecurityCenter ou usar recursos adicionais:

- Clique com o botão direito no ícone principal do SecurityCenter e clique em uma das seguintes opções:
  - Abrir o SecurityCenter
  - Atualizações
  - Links rápidos

    O submenu contém links para Início, Exibir eventos recentes, Gerenciar rede, Manter o computador e para o Data Backup (se estiver instalado).
  - Verificar assinatura

    (Esse item aparece quando a assinatura de ao menos um produto tiver expirado.)
  - Centro de Upgrade
  - Suporte ao cliente

Verifique o status de proteção

Quando o computador não está totalmente protegido, o ícone do status de proteção aparece na área de notificação do Windows, na extrema direita da barra de tarefas. O ícone pode ser amarelo ou vermelho, dependendo do status de proteção.

Para verificar o status de proteção:

- Clique no ícone do status de proteção para abrir o SecurityCenter e corrigir qualquer problema.

Verifique o status das atualizações

Quando o você verifica atualizações, o ícone de atualização aparece na área de notificação do Windows, na extrema direita da barra de tarefas.

Para verificar o status das atualizações:

- Aponte para o ícone de atualizações para exibir o status de suas atualizações em uma dica.

Noções básicas sobre o status de proteção

O status de proteção de segurança geral do computador é mostrado em **Estou protegido?** no SecurityCenter.

O status de proteção informa se o computador está totalmente protegido contra as ameaças à segurança mais recentes ou se os problemas requerem atenção e como resolvê-los. Quando um problema afeta mais de uma categoria de proteção, a correção do problema pode fazer com que várias categorias retornem ao status de proteção total.

Alguns dos fatores que influenciam o status de proteção são ameaças externas à segurança, os produtos de segurança instalados no computador, produtos que acessam a Internet e a forma como esses produtos de segurança e de Internet estão configurados.

Por padrão, se a Proteção contra spam ou o Bloqueio de conteúdo não estiverem instalados, esses problemas de proteção menos importantes serão ignorados automaticamente e não serão rastreados no status de proteção geral. Porém, se um problema de proteção for seguido de um link **Ignorar**, você poderá optar por ignorar o problema, se tiver certeza de que não deseja corrigi-lo.

Estou protegido?

Consulte o nível geral do status de proteção do computador em **Estou protegido?** no SecurityCenter:

- A mensagem **Sim** será exibida se seu computador estiver totalmente protegido (verde).
- A mensagem **Não** será exibida se seu computador estiver parcialmente protegido (amarelo) ou não estiver protegido (vermelho).

Para resolver automaticamente a maioria dos problemas de proteção , clique em **Corrigir** ao lado do status de proteção. Porém, se um ou mais problemas persistirem e exigirem sua resposta, clique no link exibido junto ao problema para adotar a ação sugerida.

Noções básicas sobre as categorias e tipos de proteção

Em **Estou protegido?** no SecurityCenter, você pode exibir uma análise do status consistindo nos seguintes tipos e categorias de proteção:

- Computador e arquivos
- Internet e rede
- E-mail e mensagens instantâneas
- Controles pelos pais

Os tipos de proteção exibidos no SecurityCenter dependem de quais produtos estão instalados. Por exemplo, o tipo de proteção PC Health é exibido se o software McAfee Data Backup estiver instalado.

Se uma categoria não tiver problemas de proteção, o status será verde. Se você clicar em uma categoria verde, uma lista dos tipos de proteção ativados será exibida à direita, seguida de uma lista de problemas já ignorados. Se não houver nenhum problema, um comunicado sobre o vírus será exibido no lugar dos problemas. Você também pode clicar em **Configurar** para alterar as opções para essa categoria.

Se todos os tipos de proteção em uma categoria tiverem status verde, então o status da categoria será verde. Do mesmo modo, se todas as categorias de proteção tiverem status verde, então o Status de proteção geral será verde.

Se alguma das categorias de proteção tiver status amarelo ou vermelho, você poderá resolver os problemas de proteção corrigindo-os ou ignorando-os e, assim, o status será alterado para verde.

Noções básicas sobre a proteção para Computador e arquivos

A categoria de proteção Computador e arquivos consiste nos seguintes tipos de proteção:

- **Proteção contra vírus** -- A proteção da varredura em tempo real defende o computador contra vírus, worms, cavalos de Tróia, scripts suspeitos, ataques híbridos e outras ameaças. Ela faz a varredura automaticamente e tenta limpar arquivos (inclusive arquivos .exe compactados, arquivos do setor de inicialização, da memória e arquivos importantes) quando são acessados por você ou pelo computador.
- **Proteção contra spyware** -- A proteção contra spyware detecta, bloqueia e remove rapidamente spyware, adware e outros programas potencialmente indesejados que podem coletar e transmitir os seus dados particulares sem a sua permissão.
- **SystemGuards** -- Os SystemGuards detectam alterações em seu computador e alertam você quando elas ocorrem. Você pode conferir essas alterações e decidir permiti-las ou não.
- **Proteção do Windows** -- A proteção do Windows informa o status do Windows Update em seu computador. Se o McAfee VirusScan estiver instalador, a proteção contra a sobrecarga do buffer também estará disponível.

Um dos fatores que influenciam a proteção Computador e arquivos é a ameaça externa de vírus. Por exemplo, se ocorrer uma epidemia de vírus, o seu software antivírus o protegerá? Além disso, há outros fatores, dentre eles a configuração do software antivírus e se o software é atualizado continuamente com os arquivos de detecção de assinatura mais recentes, para proteger o computador das últimas ameaças.

Abrir o painel de configuração Computador e arquivos

Quando não houver problemas em **Computador & arquivos**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel de configuração Computador e arquivos:

1. No painel Início, clique em **Computador & arquivos**.
2. No painel direito, clique em **Configurar**.

Noções básicas sobre a proteção de Internet e rede

A categoria de proteção Internet e rede consiste nos seguintes tipos de proteção:

- **Proteção de firewall** -- A proteção de firewall defende o computador contra invasão e tráfego de rede não desejado. Ela ajuda a gerenciar conexões de entrada e de saída com a Internet.
- **Wireless Protection** -- A Wireless Protection defende a rede sem fio doméstica contra intrusão e interceptação de dados. No entanto, se, no momento, você estiver conectado a uma rede sem fio externa, a proteção deve variar com base no nível de segurança dessa rede.
- **Proteção de navegação na Web** -- A proteção da navegação da Web oculta anúncios, pop-ups e Web bugs em seu computador quando você navega pela Internet.
- **Proteção contra phishing** -- A proteção contra phishing ajuda a bloquear sites fraudulentos que solicitam informações pessoais por meio de hiperlinks em e-mails, mensagens instantâneas, pop-ups e outras fontes.
- **Proteção de informações pessoais** -- A proteção de informações pessoais bloqueia a divulgação de informações importantes e confidenciais pela Internet.

Abrir o painel de configuração de Internet e rede

Quando não houver problemas em **Internet & rede**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel configuração de Internet e rede:

1. No painel Início, clique em **Internet & rede**.
2. No painel direito, clique em **Configurar**.

Noções básicas sobre a proteção E-mail e MI

A categoria de proteção E-mail e MI consiste nos seguintes tipos de proteção:

- **Proteção de e-mail** -- A proteção de e-mail faz a varredura automaticamente e tenta limpar vírus, spyware e ameaças potenciais em e-mails de entrada e de saída e em anexos.
- **Proteção contra spam** -- A proteção contra spam ajuda a bloquear a entrada de mensagens de e-mail indesejadas em sua caixa de entrada.
- **Proteção de MI** -- A proteção para mensagens instantâneas (MI) faz a varredura automaticamente e tenta limpar vírus, spyware e ameaças potenciais em anexos de mensagens instantâneas de entrada. Ela também impede que clientes de mensagens instantâneas compartilhem conteúdo indesejado ou informações pessoais na Internet.
- **Proteção para navegação segura** -- Quando instalado, o plug-in para navegador do McAfee SiteAdvisor ajuda a proteger contra spyware, spam, vírus e golpes on-line, classificando sites da Web que você visita ou que aparecem em seus resultados de pesquisa na Web. Você pode exibir classificações de segurança detalhadas para mostrar os resultados dos testes do site em relação a práticas de e-mail, downloads, afiliações on-line e inconvenientes como pop-ups e cookies de rastreamento de terceiros.

Abrir o painel de configuração de E-mail e MI

Quando não houver problemas em **E-mail & MI**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel de configuração de E-mail e MI:

1. No painel Início, clique em **E-mail & MI**.
2. No painel direito, clique em **Configurar**.

Noções básicas sobre a proteção Controles pelos pais

A categoria de proteção Controles pelos pais consiste no seguinte tipo de proteção:

- **Controles pelos pais** -- O Bloqueio de conteúdo impede que usuários exibam conteúdo indesejado da Internet, bloqueando sites da Web potencialmente mal-intencionados. O uso e as atividades na Internet dos usuários também podem ser monitorados e limitados.

Abrir o painel de configuração Controles pelos pais

Quando não houver problemas em **Controles pelos pais**, você poderá abrir o painel de configuração a partir do painel de informações.

Para abrir o painel de configuração Controles pelos pais:

1. No painel Início, clique em **Controles pelos pais**.
2. No painel direito, clique em **Configurar**.

Corrigindo problemas de proteção

A maior parte dos problemas de proteção pode ser resolvida automaticamente. Porém, se um ou mais problemas persistirem, você deverá resolvê-los.

Corrigir problemas de proteção automaticamente

A maior parte dos problemas de proteção pode ser resolvida automaticamente.

Para corrigir problemas de proteção automaticamente:

- Clique em **Corrigir**, ao lado do status de proteção.

Corrigir problemas de proteção manualmente

Se um ou mais problemas de proteção não forem resolvidos automaticamente, clique no link ao lado do problema para adotar a ação sugerida.

Para corrigir problemas de proteção manualmente:

- Escolha uma das seguintes opções:
  - Se não tiver sido feita uma varredura completa de seu computador nos últimos 30 dias, clique em **Varredura** à esquerda do status de proteção principal, para realizar uma varredura manual. (Esse item aparecerá se o McAfee VirusScan estiver instalado.)
  - Se os seus arquivos de detecção de assinatura (DAT) estiverem desatualizados, clique no link **Atualizar**, à esquerda do status de proteção principal, para atualizar sua proteção.
  - Se o programa não estiver instalado, clique em **Obter proteção total** para instalá-lo.
  - Se um programa estiver com componentes faltantes, reinstale-o.
  - Se um programa precisar ser registrado para receber proteção total, clique em **Registrar agora**, para registrá-lo. (Esse item aparece quando um ou mais programas expiraram.)
  - Se um programa expirar, clique em **Verificar minha assinatura agora**, para verificar o status de sua conta. (Esse item aparece quando um ou mais programas expiraram.)

Exibindo informações do SecurityCenter

Na parte inferior do painel de status de proteção, as Informações do SecurityCenter fornecem acesso às opções do SecurityCenter e mostram a última atualização, a última varredura (se o McAfee VirusScan estiver instalado) e informações sobre expiração de assinatura dos produtos McAfee.

Abra o painel de configuração do SecurityCenter

Para maior praticidade, você pode abrir o painel de configuração do SecurityCenter para alterar as opções, a partir do painel Início.

Para abrir o painel de configuração do SecurityCenter:

- No painel Início, em **Informações do SecurityCenter**, clique em **Configurar**.

Exiba as informações do produto instalado

Você pode exibir uma lista de produtos instalados que mostra o número da versão do produto e a data da última atualização.

Para exibir as informações do produto McAfee:

- No painel Início, em **Informações do SecurityCenter**, clique em **Exibir detalhes** para abrir a janela de informações do produto.

Usando o Menu avançado

Quando o SecurityCenter é aberto pela primeira vez, o Menu básico aparece na coluna à esquerda. Se você for um usuário avançado, pode clicar no **Menu avançado** para abrir um menu de comandos mais detalhado no lugar desse. Para maior praticidade, o último menu usado será mostrado dá próxima vez que você abrir o SecurityCenter.

O Menu avançado contém os seguintes itens:

- Início
- Relatórios e registros (inclui a lista de Eventos recentes e registros por tipo dos últimos 30, 60 e 90 dias)
- Configurar
- Restaurar
- Ferramentas

CAPÍTULO 4

Configurando opções do SecurityCenter

O SecurityCenter mostra o status de proteção de segurança geral do computador, permite criar contas de usuário McAfee, instala automaticamente as atualizações mais recentes do produto e notifica você automaticamente, com alertas e sons, sobre epidemias públicas de vírus, ameaças à segurança e atualizações do produto.

No painel de configuração do SecurityCenter, é possível alterar as opções do SecurityCenter para os seguintes recursos:

- Status de proteção
- Usuários
- Atualizações automáticas
- Alertas

Neste capítulo

Configurando o status de proteção

O status de proteção de segurança geral do computador é mostrado em **Estou protegido?** no SecurityCenter.

O status de proteção informa se o computador está totalmente protegido contra as ameaças à segurança mais recentes ou se os problemas requerem atenção e como resolvê-los.

Por padrão, se a Proteção contra spam ou o Bloqueio de conteúdo não estiverem instalados, esses problemas de proteção menos importantes serão ignorados automaticamente e não serão rastreados no status de proteção geral. Porém, se um problema de proteção for seguido de um link **Ignorar**, você poderá optar por ignorar o problema, se tiver certeza de que não deseja corrigi-lo. Se, posteriormente, decidir corrigir um problema ignorado anteriormente, você poderá incluí-lo no status de proteção para rastreamento.

Configurar problemas ignorados

Você pode incluir ou excluir problemas do rastreamento como parte do status de proteção geral do computador. Se um problema de proteção for seguido por um link **Ignorar**, você poderá optar por ignorar o problema, se tiver certeza de que não deseja corrigi-lo. Se, posteriormente, decidir corrigir um problema ignorado anteriormente, você poderá incluí-lo no status de proteção para rastreamento.

Para configurar problemas ignorados:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Status de proteção** para expandir o painel e clique em **Avançado**.

3 Realize uma das seguintes ações no painel Problemas ignorados:

   - Para incluir problemas ignorados anteriormente no status de proteção, desmarque suas caixas de seleção.
   - Para excluir problemas do status de proteção, selecione suas caixas de seleção.

4 Clique em **OK**.

Configurando opções do usuário

Se você estiver executando programas da McAfee que exigem permissões de usuário, essas permissões corresponderão, por padrão, às contas de usuário do Windows em seu computador. Para facilitar o gerenciamento de usuários para esses programas, você pode alternar para usar contas de usuário da McAfee a qualquer momento.

Se você alternar para as contas de usuário da McAfee, todos os nomes de usuário e permissões existentes no programa Controles pelos pais serão importados automaticamente. No entanto, na primeira vez em que você alterna, é necessário criar uma Conta de administrador. Depois disso, você pode começar a criar e configurar outras contas de usuário da McAfee.

Alternar para contas de usuário da McAfee

Por padrão, você usa contas de usuário do Windows. No entanto, alternar para contas de usuário da McAfee faz com que seja desnecessário criar contas adicionais de usuário do Windows.

Para alternar para contas de usuário da McAfee:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Usuários** para expandir o painel e clique em **Avançado**.

3 Para usar contas de usuário da McAfee, clique em **Alternar**.

Caso esteja alternando para contas de usuário da McAfee pela primeira vez, você deve criar uma Conta de administrador (página 24).

Criar uma Conta de administrador

Na primeira vez em que alternar para utilizar usuários da McAfee, você receberá uma solicitação para criar uma Conta de administrador.

Para criar uma Conta de administrador:

1 Digite uma senha na caixa **Senha** e digite-a novamente na caixa **Confirmar senha**.

2 Selecione uma pergunta de recuperação de senha da lista e digite a resposta à pergunta secreta na caixa **Resposta**.

3 Clique em **Aplicar**.

   Quando você concluir, o tipo de conta do usuário estará atualizado no painel, com os nomes de usuário e as permissões existentes do programa Controles pelos pais, se houver. Se você estiver configurando contas de usuário pela primeira vez, o painel Gerenciar usuários será exibido.

Configurar opções do usuário

Se você alternar para as contas de usuário da McAfee, todos os nomes de usuário e permissões existentes no programa Controles pelos pais serão importados automaticamente. No entanto, na primeira vez em que você alterna, é necessário criar uma Conta de administrador. Depois disso, você pode começar a criar e configurar outras contas de usuário da McAfee.

Para configurar opções do usuário:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta ao lado de **Usuários** para expandir o painel e clique em **Avançado**.
3. Em **Contas de usuário**, clique em **Adicionar**.
4. Digite um nome de usuário na caixa **Nome do usuário**.
5. Digite uma senha na caixa **Senha** e digite-a novamente na caixa **Confirmar senha**.
6. Selecione a caixa **Usuário de inicialização**, se desejar que este usuário efetue logon automaticamente quando o SecurityCenter for iniciado.
7. Em **Tipo de conta de usuário**, selecione um tipo de conta para este usuário e clique em **Criar**.

   Observação: Após criar a conta de usuário, você deve definir as configurações para um Usuário limitado em Controles pelos pais.

8. Para editar a senha, o logon automático ou o tipo de conta de um usuário, selecione um nome de usuário na lista e clique em **Editar**.
9. Ao terminar, clique em **Aplicar**.

Recuperar a Senha de administrador

Caso esqueça a Senha do administrador, você poderá recuperá-la.

Para recuperar a senha de administrador:

1. Clique com o botão direito do mouse no ícone M do SecurityCenter e clique em **Alternar usuário**.
2. Na lista **Nome do usuário**, selecione **Administrador** e clique em **Esqueceu a senha?**.
3. Digite a resposta à pergunta secreta que você selecionou ao criar a Conta do administrador.
4. Clique em **Enviar**.

   A Senha do administrador esquecida será exibida.

Alterar a Senha do administrador

Caso não consiga lembrar a Senha do administrador ou suspeite que ela esteja comprometida, você pode alterá-la.

Para alterar a Senha do administrador:

1 Clique com o botão direito do mouse no ícone M do SecurityCenter e clique em **Alternar usuário**.

2 Na lista **Nome do usuário**, selecione **Administrador** e clique em **Alterar senha**.

3 Digite a senha atual na caixa **Senha antiga**.

4 Digite sua nova senha na caixa **Senha**, e digite-a novamente na caixa **Confirmar senha**.

5 Clique em **OK**.

Configurando opções de atualização

O McAfee SecurityCenter verifica automaticamente se há atualizações para todos os serviços McAfee a cada quatro horas, quando você está conectado à Internet, instalando automaticamente as atualizações mais recentes do produto. Porém, você pode verificar atualizações manualmente a qualquer momento, usando o ícone do SecurityCenter na área de notificação na extrema direita da barra de tarefas.

Verificar atualizações automaticamente

O SecurityCenter verifica automaticamente as atualizações a cada quatro horas quando você está conectado à Internet. No entanto, você pode configurar o SecurityCenter para notificar você antes de fazer download ou instalar atualizações.

Para verificar atualizações automaticamente:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta ao lado do status de **Atualizações automáticas ativadas** para expandir o painel e clique em **Avançado**.
3. Selecione uma das opções a seguir, no painel Opções de atualização:
   - Instalar as atualizações automaticamente e notificar-me quando o produto estiver atualizado (recomendável) (página 28)
   - Fazer o download das atualizações automaticamente e notificar-me quando estiverem prontas para serem instaladas (página 29)
   - Notificar-me antes de fazer o download de atualizações (página 29)
4. Clique em **OK**.

Observação: Para obter proteção máxima, a McAfee recomenda que você deixe o SecurityCenter verificar e instalar as atualizações automaticamente. Entretanto, se desejar atualizar apenas manualmente os serviços de segurança, você poderá desativar a atualização automática (página 30).

Fazer o download e a instalação das atualizações automaticamente

Se você selecionar **Instalar as atualizações automaticamente e notificar-me quando meus serviços forem atualizados (recomendável)**, nas Opções de atualização do SecurityCenter, o SecurityCenter fará o download e a instalação das atualizações automaticamente.

Fazer o download de atualizações automaticamente

Se você selecionar **Fazer o download das atualizações automaticamente e notificar-me quando estiverem prontas para ser instaladas** em Opções de atualização, o SecurityCenter fará o download das atualizações automaticamente e irá notificá-lo quando estiverem prontas para ser instaladas. Você pode optar por instalar ou adiar a atualização (página 30).

Para instalar uma atualização obtida por download automaticamente:

1 Clique em **Atualizar meus produtos agora** no alerta e clique em **OK**.

   Se solicitado, você deverá efetuar logon no site da Web para que sua assinatura seja verificada, antes de fazer o download.

2 Depois de verificar a assinatura, clique em **Atualizar** no painel Atualizações para fazer o download e instalar a atualização. Se a assinatura tiver expirado, clique em **Renovar minha assinatura** no alerta e siga as instruções.

Observação: Em alguns casos, você será solicitado a reiniciar o computador para concluir a atualização. Salve todo o seu trabalho e feche todos os programas antes de reiniciar.

Notificar antes de fazer o download das atualizações

Se você selecionar **Notificar-me antes de fazer o download de atualizações** no painel Opções de atualização, o SecurityCenter irá notificá-lo antes de fazer o download de qualquer atualização. Você pode optar por fazer o download e a instalação de uma atualização nos serviços de segurança para eliminar uma ameaça de ataque.

Para fazer o download e a instalação de uma atualização:

1 Selecione **Atualizar meus produtos agora** no alerta e clique em **OK**.

2 Se solicitado, efetue logon no site da Web.

   O download de atualização é feito automaticamente.

3 Clique em **OK** no alerta quando a instalação da atualização estiver concluída.

Observação: Em alguns casos, você será solicitado a reiniciar o computador para concluir a atualização. Salve todo o seu trabalho e feche todos os programas antes de reiniciar.

Desativar a atualização automática

Para obter proteção máxima, a McAfee recomenda que você deixe o SecurityCenter verificar e instalar as atualizações automaticamente. Entretanto, se desejar atualizar apenas manualmente os serviços de segurança, você poderá desativar a atualização automática.

Observação: Você deve lembrar-se de verificar as atualizações manualmente (página 31) pelo menos uma vez por semana. Se você não verificar se há atualizações, seu computador não estará protegido pelas atualizações de segurança mais recentes .

Para desativar a atualização automática:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta ao lado do status de **Atualizações automáticas ativadas** para expandir o painel.
3. Clique em **Desligado**.
4. Clique em **Sim** para confirmar a alteração.

   O status é atualizado no cabeçalho.

Se você não verificar as atualizações manualmente em sete dias, é emitido um alerta para lembrá-lo.

Adiar atualizações

Se você não puder atualizar os serviços de segurança quando o alerta for exibido, poderá optar por ser lembrado posteriormente ou ignorar o alerta.

Para adiar uma atualização:

- Escolha uma das seguintes opções:
  - Selecione **Lembre-me mais tarde** no alerta e clique em **OK**.
  - Selecione **Fechar este alerta** e clique em **OK** para fechar o alerta sem executar nenhuma ação.

Verificar atualizações manualmente

O SecurityCenter verifica automaticamente se há atualizações a cada quatro horas quando você está conectado à Internet e, em seguida, instala as atualizações mais recentes do produto. Porém, você pode verificar atualizações manualmente a qualquer momento, usando o ícone do SecurityCenter na área de notificação do Windows, na extrema direita da barra de tarefas.

Observação: Para obter proteção máxima, a McAfee recomenda que você deixe o SecurityCenter verificar e instalar as atualizações automaticamente. Entretanto, se desejar atualizar apenas manualmente os serviços de segurança, você poderá desativar a atualização automática (página 30).

Para verificar manualmente se existem atualizações:

1 Verifique se o computador está conectado à Internet.

2 Clique com o botão direito no ícone M do SecurityCenter na área de notificação do Windows, na extrema direita da barra de tarefas e clique em **Atualizações**.

   Enquanto o SecurityCenter está verificando as atualizações, você continuar a executar outras tarefas com ele.

   Para maior praticidade, um ícone animado é exibido na área de notificação do Windows, na extrema direita da barra de tarefas. Quando o SecurityCenter tiver terminado, o ícone desaparecerá automaticamente.

3 Se solicitado, efetue logon no site da Web para que sua assinatura seja verificada.

Observação: Em alguns casos, você será solicitado a reiniciar o computador para concluir a atualização. Salve todo o seu trabalho e feche todos os programas antes de reiniciar.

Configurando opções de alerta

O SecurityCenter notifica automaticamente, por meio de alertas e sons, sobre epidemias públicas de vírus, ameaças à segurança e atualizações do produto. Porém, você pode configurar o SecurityCenter para mostrar somente alertas que exijam atenção imediata.

Configurar opções de alerta

O SecurityCenter notifica automaticamente, por meio de alertas e sons, sobre epidemias públicas de vírus, ameaças à segurança e atualizações do produto. Porém, você pode configurar o SecurityCenter para mostrar somente alertas que exijam atenção imediata.

Para configurar as opções de alerta:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Alertas** para expandir o painel e clique em **Avançado**.

3 Selecione uma das opções a seguir no painel Opções de alerta:

- **Alertar-me quando ocorrer um surto público de um vírus ou uma ameaça à segurança**
- **Mostrar alertas informativos quando o modo de jogos for detectado**
- **Executar um som quando ocorrer um alerta**
- **Mostrar tela de abertura da McAfee ao iniciar o Windows**

4 Clique em **OK**.

Observação: Para desativar alertas informativos futuros a partir do próprio alerta, selecione a caixa **Não mostrar este alerta novamente**. Você pode ativá-lo novamente mais tarde no painel Alertas informativos.

Configurar alertas informativos

Os alertas informativos avisam você quando ocorrem eventos que não exigem resposta imediata. Se você desativar alertas informativos futuros a partir do próprio alerta, você poderá ativá-los novamente mais tarde no painel Alertas informativos.

Para configurar alertas informativos:

1 Em **Informações do SecurityCenter**, clique em **Configurar**.

2 Clique na seta ao lado de **Alertas** para expandir o painel e clique em **Avançado**.

3 Em **Configuração do SecurityCenter**, clique em **Alertas informativos**.

4 Desmarque a caixa de seleção **Ocultar alertas informativos** e, em seguida, desmarque as caixas de seleção dos alertas da lista que você deseja mostrar.

5 Clique em **OK**.

CAPÍTULO 5

Executando tarefas comuns

Você pode executar tarefas comuns, incluindo retornar ao painel Início, exibir eventos recentes, gerenciar a rede do computador (se for um computador com recursos de gerenciamento para esta rede) e manutenção do computador. Se o McAfee Data Backup estiver instalado, você também poderá fazer backup de dados.

Neste capítulo

Executar tarefas comuns

Você pode executar tarefas comuns, incluindo retornar ao painel Início, exibir eventos recentes, fazer a manutenção do computador, gerenciar a rede (se for um computador com recursos de gerenciamento para esta rede), além de fazer backup de dados (se o McAfee Data Backup estiver instalado).

Para executar tarefas comuns:

- Em **Tarefas comuns** no Menu básico, execute um dos procedimentos a seguir:
  - Para retornar ao painel Início, clique em **Início**.
  - Para exibir eventos recentes detectados por seu software de segurança, clique em **Eventos recentes**.
  - Para remover arquivos não utilizados, desfragmentar dados e restaurar as configurações anteriores do computador, clique em **Manter o computador**.
  - Para gerenciar a rede do computador, clique em **Gerenciar rede**, em um computador com recurso de gerenciamento para esta rede.

    O Network Manager monitora as falhas de segurança dos computadores em sua rede para que você possa identificar problemas de segurança de rede facilmente.
  - Para criar cópias de backup de seus arquivos, clique em **Data Backup**, se o McAfee Data Backup estiver instalado.

O backup automático salva cópias de seus arquivos mais valiosos onde você desejar, criptografando e armazenando os arquivos em um CD/DVD, em uma unidade USB, externa ou de rede.

Dica: Para maior praticidade, você pode realizar tarefas comuns a partir de dois outros locais (em **Início**, no Menu avançado, e no menu **QuickLinks** do ícone M do SecurityCenter, na extrema direita da barra de tarefas). Também é possível exibir eventos recentes e registros abrangentes por tipo em **Relatórios e registros**, no Menu avançado.

Exibir eventos recentes

Eventos recentes são registrados quando ocorrem alterações no computador. Isso ocorre, por exemplo, quando um tipo de proteção é ativado ou desativado, quando uma ameaça é removida ou quando a tentativa de conexão com a Internet é bloqueada. Você pode exibir os 20 eventos mais recentes e seus detalhes.

Consulte o arquivo da Ajuda do produto em questão para obter detalhes sobre seus eventos.

Para exibir eventos recentes:

1 Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, e clique em **Exibir eventos recentes**.

   Todos os eventos recentes aparecerão na lista, mostrando a data e uma descrição breve.

2 Em **Eventos recentes**, selecione um evento para exibir informações adicionais no painel Detalhes.

   Em **Desejo**, serão exibidas as ações disponíveis.

3 Para exibir uma lista mais abrangente de eventos, clique em **Exibir registro**.

Fazer a manutenção do computador automaticamente

Para liberar um espaço valioso na unidade e otimizar o desempenho do computador, você pode programar as tarefas QuickClean ou Desfragmentador de disco para que sejam executadas em intervalos regulares. Essas tarefas incluem exclusão, destruição e desfragmentação de arquivos e pastas.

Para fazer a manutenção do computador automaticamente:

1. Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, em seguida, clique em **Manter o computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.
3. Na lista de operação, selecione **QuickClean** ou **Desfragmentador de disco**.
4. Escolha uma das seguintes opções:
   - Para modificar uma tarefa existente, selecione-a e clique em **Modificar**. Siga as instruções da tela.
   - Para criar uma nova tarefa, digite o nome na caixa **Nome da tarefa** e clique em **Criar**. Siga as instruções da tela.
   - Para excluir uma tarefa, selecione-a e clique em **Excluir**.
5. Em **Resumo da tarefa**, veja quando a tarefa foi executada pela última vez, quando será executada novamente e seu status.

Fazer a manutenção do computador manualmente

Você pode executar tarefas manuais de manutenção para remover arquivos não utilizados, desfragmentar seus dados ou restaurar as configurações anteriores do computador.

Para fazer a manutenção do computador manualmente:

- Escolha uma das seguintes opções:
  - Para usar o QuickClean, clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, clique em **Manter o computador** e, em seguida, clique em **Iniciar**.
  - Para usar o Desfragmentador de disco, clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, clique em **Manter o computador**.e, em seguida, clique em **Analisar**.
  - Para usar a Restauração de sistema , no Menu avançado, clique em **Ferramentas**, **Restauração do sistema** e, em seguida, clique em **Iniciar**.

Remover arquivos e pastas não utilizados

Use o QuickClean para liberar um espaço valioso na unidade e otimizar o desempenho do computador.

Para remover arquivos e pastas não utilizados:

1. Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, em seguida, clique em **Manter o computador**.
2. Em **QuickClean**, clique em **Iniciar**.
3. Siga as instruções da tela.

Desfragmentar arquivos e pastas

A fragmentação de arquivos ocorre quando arquivos e pastas são excluídos e novos arquivos são adicionados. Essa fragmentação torna o acesso ao disco mais lento e prejudica o desempenho geral do computador, embora não de forma grave, normalmente.

Use a desfragmentação para regravar partes de um arquivo para setores contíguos em um disco rígido, de modo a aumentar a velocidade de acesso e recuperação.

Para desfragmentar arquivos e pastas:

1 Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks**, e clique em **Manter o computador**.

2 Em **Desfragmentador de disco**, clique em **Analisar**.

3 Siga as instruções da tela.

Restaurar as configurações anteriores do computador

Pontos de restauração são instantâneos do computador que o Windows salva periodicamente e quando ocorrem eventos significativos (como a instalação de um programa ou unidade). Porém, você pode criar e nomear seus próprios pontos de restauração a qualquer momento.

Use pontos de restauração para desfazer alterações nocivas no computador e retornar às configurações anteriores.

Para restaurar as configurações anteriores do computador:

1 No Menu avançado, clique em **Ferramentas** e clique em **Restauração do sistema**.

2 Em **Restauração do sistema**, clique em **Iniciar**.

3 Siga as instruções da tela.

Gerenciar a rede

Se o computador tiver recursos de gerenciamento para sua rede, você poderá usar o Network Manager para monitorar computadores em toda a rede para identificar problemas de segurança de rede facilmente.

Se o status de proteção do computador não estiver sendo monitorado nesta rede, então o computador não pertence à rede ou é um membro não gerenciado da rede. Consulte detalhes no arquivo da Ajuda do Network Manager.

Para gerenciar sua rede:

1 Clique com o botão direito no ícone do SecurityCenter, aponte para **QuickLinks** e clique em **Gerenciar rede**.

2 Clique no ícone que representa este computador no mapa da rede.

3 Em **Desejo**, clique em **Monitorar este computador**.

Saiba mais sobre vírus

Use a Biblioteca de informações sobre vírus e o Virus Map e:

- Saiba mais sobre os mais recentes vírus, embustes de vírus em e-mail e outras ameaças.
- Obtenha ferramentas gratuitas de remoção de vírus para ajudar a reparar seu computador.
- Obtenha uma visão geral em tempo real dos locais em que os vírus mais recentes estão infectando computadores no mundo todo.

Para saber mais sobre vírus:

1 No Menu avançado, clique em **Ferramentas** e clique em **Informações sobre vírus**.

2 Escolha uma das seguintes opções:

   - Pesquise vírus usando a Biblioteca de informações sobre vírus gratuita da McAfee.
   - Pesquise vírus usando o World Virus Map no site da McAfee na Web.

CAPÍTULO 6

McAfee QuickClean

Resíduos se acumulam rapidamente em seu computador ao navegar na Internet. Com o QuickClean, você protege a sua privacidade e exclui os resíduos de Internet e de e-mail que não são necessários. O QuickClean identifica e exclui os arquivos que se acumulam durante a navegação, incluindo cookies, e-mails, downloads e históricos—dados que contêm informações pessoais sobre você. Ele protege a sua privacidade, oferecendo exclusão segura destas informações confidenciais.

O QuickClean também exclui programas indesejados. Especifique os arquivos que você deseja eliminar e livre-se dos resíduos sem excluir as informações essenciais.

Neste capítulo

Noções básicas sobre os recursos do QuickClean

Esta seção descreve os recursos do QuickClean.

Recursos

O QuickClean fornece um conjunto de ferramentas eficientes e de fácil utilização que exclui com segurança os fragmentos digitais. Você pode liberar um valioso espaço na unidade e otimizar o desempenho do seu computador.

CAPÍTULO 7

Limpando o computador

O QuickClean permite excluir com segurança os arquivos e as pastas.

Ao navegar na Internet, seu navegador copia cada página da Internet e seus gráficos para uma pasta em cache em seu disco. O navegador então pode carregar a página rapidamente, se você voltar a visitá-la. Armazenar os arquivos em cache é útil se você visita várias vezes as mesmas páginas da Internet e se os conteúdos das páginas não são alterados com freqüência. No entanto, na maioria das vezes, os arquivos em cache não são úteis e podem ser excluídos.

Você pode excluir diversos itens com os seguintes limpadores.

- Limpador da lixeira: Limpa a sua lixeira do Windows.
- Limpador de arquivos temporários: Exclui os arquivos armazenados nas pastas temporárias.
- Limpador de atalhos: Exclui os atalhos quebrados e os atalhos sem um programa associado.
- Limpador de fragmentos perdidos de arquivos: Exclui os fragmentos de arquivos perdidos de seu computador.
- Limpador de registro: Exclui as informações do Registro do Windows para programas que não existem mais em seu computador.
- Limpador de cache: Exclui os arquivos em cache que se acumulam quando você navega na Internet. Arquivos desse tipo normalmente são armazenados como arquivos temporários da Internet.
- Limpador de cookies: Exclui os cookies. Arquivos desse tipo normalmente são armazenados como arquivos temporários da Internet.
  Os cookies são arquivos pequenos que o navegador da Web armazena no computador atendendo a uma solicitação do servidor Web. Toda vez que você exibir uma página da Web do servidor Web, o navegador enviará o cookie de volta ao servidor. Esses cookies podem agir como uma marca, permitindo que o servidor Web rastreie as páginas que foram exibidas e a freqüência na qual você volta nelas.
- Limpador de histórico do navegador: Exclui seu histórico de navegador.
- Limpador de e-mails do Outlook Express e do Outlook para itens excluídos e enviados: Exclui o correio das pastas Enviadas e Excluídas do Outlook.

- Limpador usado recentemente: Exclui os itens usados recentemente e armazenados em seu computador, como documentos do Microsoft Office.
- Limpador de ActiveX e de plug-in: Exclui controles e plug-ins do ActiveX.
  O ActiveX é uma tecnologia usada para implementar os controles em um programa. Um controle ActiveX pode adicionar um botão à interface de um programa. A maioria desses controles são inofensivos; no entanto, algumas pessoas podem usar a tecnologia ActiveX para capturar as informações de seu computador.
  Os plug-ins são pequenos programas de software que se conectam a aplicativos maiores para fornecer funcionalidade adicional. Plug-ins permitem que o navegador da Web acesse e execute os arquivos incorporados nos documentos HTML que estejam em formatos que o navegador normalmente não reconheceria (por exemplo, animação, vídeo e arquivos de áudio).
- Limpador do ponto de restauração do sistema: Exclui os antigos pontos de restauração do sistema do seu computador.

Neste capítulo

Usando o QuickClean

Esta seção descreve como utilizar o QuickClean.

Limpe o seu computador

Você pode excluir arquivos e pastas não usados, liberar espaço em disco e permitir que seu computador seja executado com mais eficiência.

Para limpar o seu computador:

1. No menu Avançado, clique em **Ferramentas**.
2. Clique em **Manter o computador** e, em seguida, clique em **Iniciar** em **McAfee QuickClean**.
3. Escolha uma das seguintes opções:
   - Clique em **Avançar** para aceitar os limpadores padrão na lista.
   - Selecione ou desmarque os limpadores apropriados e, em seguida, clique em **Avançar.** Para o Limpador usado recentemente, você pode clicar em **Propriedades** para desmarcar os programas cujas listas você não deseja limpar.
   - Clique em **Restaurar padrões** para restaurar os limpadores padrão e, em seguida, clique em **Avançar.**
4. Depois que a análise for executada, clique em **Avançar** para confirmar a exclusão do arquivo. Você pode expadir essa lista para ver os arquivos que serão limpos e seus locais.
5. Clique em **Avançar.**
6. Escolha uma das seguintes opções:
   - Clique em **Avançar** para aceitar o padrão **Não, desejo excluir os arquivos usando a exclusão padrão do Windows**.
   - Clique em **Sim, desejo apagar com segurança os meus arquivos usando o Shredder** e especificar o número de etapas. Arquivos excluídos com o Shredder não podem ser recuperados.
7. Clique em **Concluir**.
8. Em **Resumo do QuickClean**, exiba o número de arquivos de Registro que foram excluídos e a quantidade de espaço em disco recuperada após a limpeza do disco e da Internet.

CAPÍTULO 8

McAfee Shredder

Os arquivos excluídos podem ser recuperados no seu computador até mesmo depois do esvaziamento da Lixeira. Quando um arquivo é excluído, o Windows marca esse espaço na unidade de disco para indicar que ele não está mais sendo utilizado, mas o arquivo continua presente. Usando ferramentas de análise legal do computador, você pode recuperar registros de impostos, currículos ou outros documentos que tenham sido excluídos. O Shredder protege a sua privacidade, excluindo os arquivos indesejados de forma segura e permanente.

Para excluir um arquivo permanentemente, é preciso sobrescrever várias vezes o arquivo existente com novos dados. O Microsoft® Windows não exclui os arquivos com segurança, porque cada operação de arquivo seria muito lenta. A destruição de um documento nem sempre impede que ele seja recuperado, pois alguns programas fazem cópias ocultas temporárias de documentos abertos. Se você destruiu apenas os documentos exibidos no Windows® Explorer, ainda pode haver cópias temporárias desses documentos.

Observação: Não é feito o backup dos arquivos destruídos. Você não pode restaurar os arquivos que o Shredder excluiu.

Neste capítulo

Noções básicas dos recursos do Shredder

Esta seção descreve os recursos do Shredder.

Recursos

O Shredder permite apagar o conteúdo da Lixeira, os arquivos temporários da Internet, o histórico do site da Web, os arquivos, as pastas e os discos.

CAPÍTULO 9

Apagando arquivos indesejados com o Shredder

O Shredder protege a sua privacidade, excluindo de forma segura e permanente os arquivos indesejados, como o conteúdo da Lixeira, os arquivos temporários da Internet e o histórico do site da Web. Você pode selecionar os arquivos e as pastas a serem destruídos ou procurar por eles.

Neste capítulo

Usando o Shredder

Esta seção descreve como utilizar o Shredder.

Arquivos, pastas e discos destruídos

Os arquivos podem permanecer em seu computador mesmo depois que você esvaziar a sua Lixeira. No entanto, ao destruir os arquivos, os seus dados são permanentemente excluídos e os hackers não podem acessá-los.

Para destruir arquivos, pastas e discos:

1 No menu Avançado, clique em **Ferramentas** e, em seguida, clique em **Shredder**.

2 Escolha uma das seguintes opções:

- Clique em **Apagar arquivos e pastas** para destruir os arquivos e as pastas.
- Clique em **Apagar um disco inteiro** para destruir discos**.**

3 Selecione um dos seguintes níveis de destruição:

- **Rápida**: Destrói os itens selecionados em uma única etapa.
- **Abrangente**: Destrói os itens selecionados em sete etapas.
- **Personalizada**: Destrói os itens selecionados em até dez etapas. Um número superior de etapas de destruição aumenta o nível de exclusão do arquivo de segurança.

4 Clique em **Avançar**.

5 Escolha uma das seguintes opções:

- Se você estiver destruindo arquivos, clique em **Conteúdo da Lixeira**, **Arquivos temporários da Internet** ou **Histórico do site da Web** na lista **Selecionar arquivos a serem destruídos**. Se você estiver destruindo um disco, clique no disco.
- Clique em **Procurar**, navegue até os arquivos que você deseja destruir e, em seguida, selecione-os.
- Digite o caminho até os arquivos que você deseja destruir na lista **Selecionar arquivos a serem destruídos**.

6 Clique em **Avançar**.

7 Clique em **Concluir** para concluir a operação.

8 Clique em **Concluído.**

C A P Í T U L O 1 0

McAfee Network Manager

O McAfee® Network Manager apresenta uma exibição gráfica dos computadores e componentes que fazem parte da sua rede doméstica. Você pode usar o Network Manager para monitorar remotamente o status de proteção de cada computador gerenciado da sua rede e para corrigir remotamente as vulnerabilidades de segurança reportadas nesses computadores gerenciados.

Antes de começar a usar o Network Manager, você pode se familiarizar com alguns dos recursos mais populares. A Ajuda do Network Manager fornece detalhes sobre como configurar e usar esses recursos.

Neste capítulo

Recursos

O Network Manager oferece os seguintes recursos:

Mapa gráfico da rede

O mapa de rede do Network Manager oferece uma representação gráfica do status de segurança dos computadores e componentes que fazem parte de sua rede doméstica. Quando você faz modificações na rede (adicionando um computador, por exemplo), o mapa de rede reconhece essas alterações. Você pode atualizar o mapa de rede, renomear a rede e mostrar ou ocultar componentes do mapa de rede, para personalizar sua exibição. Também é possível exibir os detalhes associados a qualquer dos componentes exibidos no mapa de rede.

Gerenciamento remoto

Use o mapa de rede do Network Manager para gerenciar o status de segurança dos computadores que fazem parte de sua rede doméstica. Você pode convidar um computador a associar-se à rede gerenciada, monitorar o status de segurança dos computadores gerenciados e corrigir vulnerabilidades de segurança conhecidas a partir de um computador remoto da rede.

Noções básicas sobre os ícones do Network Manager

A tabela a seguir descreve os ícones geralmente usados no mapa de rede do Network Manager.

Ícone	Descrição
	Representa um computador gerenciado on-line
	Representa um computador gerenciado off-line
	Representa um computador não gerenciado com o software de segurança McAfee 2007 instalado
	Representa um computador não gerenciado off-line
	Representa um computador on-line sem o software de segurança McAfee 2007 instalado ou um dispositivo de rede desconhecido
	Representa um computador off-line sem o software de segurança McAfee 2007 instalado ou um dispositivo de rede desconhecido off-line
	Significa que o item correspondente está protegido e conectado
	Significa que o item correspondente exige a sua atenção
	Significa que o item correspondente exige a sua atenção e está desconectado
	Representa um roteador doméstico sem fio
	Representa um roteador doméstico padrão
	Representa a Internet, quando conectada
	Representa a Internet, quando desconectada

CAPÍTULO 11

Configurando uma rede gerenciada

Você configura uma rede gerenciada trabalhando com os itens de seu mapa de rede e adicionando membros (computadores) a ela.

Neste capítulo

Trabalhando com o mapa de rede

Sempre que um computador é conectado à rede, o Network Manager analisa o estado da rede para determinar a presença de membros (gerenciados ou não), os atributos do roteador e o status da Internet. Se nenhum membro for encontrado, o Network Manager presume que o computador conectado atualmente é o primeiro computador da rede e automaticamente o torna um membro gerenciado com permissões administrativas. Por padrão, o nome da rede inclui o grupo de trabalho ou o domínio do primeiro computador conectado à rede com o software de segurança McAfee 2007 instalado. Contudo, você pode renomear a rede a qualquer momento.

Quando fizer modificações na rede (adicionando um computador, por exemplo), você poderá personalizar o mapa de rede. Por exemplo, você pode atualizar o mapa de rede, renomear a rede e mostrar ou ocultar componentes do mapa de rede, para personalizar sua exibição. Também é possível exibir os detalhes associados a qualquer dos componentes exibidos no mapa de rede.

Acessar o mapa de rede

Para acessar um mapa da sua rede, inicie o Network Manager a partir da lista de tarefas comuns do SecurityCenter. O mapa de rede fornece uma representação gráfica dos computadores e componentes que fazem parte da sua rede doméstica.

Para acessar o mapa de rede:

- No menu Básico ou Avançado, clique em **Gerenciar rede**.
  O mapa de rede é exibido no painel direito.

Observação: Quando acessar o mapa de rede pela primeira vez, você será solicitado a confiar nos outros computadores da rede antes que o mapa de rede seja exibido.

Atualizar o mapa de rede

Você pode atualizar o mapa da rede a qualquer momento; por exemplo, depois que outro computador associa-se à rede gerenciada.

Para atualizar o mapa de rede:

1 No menu Básico ou Avançado, clique em **Gerenciar rede**. O mapa de rede é exibido no painel direito.

2 Clique em **Atualizar o mapa de rede**, em **Desejo**.

Observação: O link **Atualizar o mapa de rede** só está disponível quando não há itens selecionados no mapa de rede. Para desmarcar um item, clique no item selecionado ou clique em uma área em branco no mapa de rede.

Renomear a rede

Por padrão, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador conectado à rede com software de segurança McAfee 2007 instalado. Se esse nome não for adequado, você poderá mudá-lo.

Para renomear a rede:

1 No menu Básico ou Avançado, clique em **Gerenciar rede**. O mapa de rede é exibido no painel direito.

2 Clique em **Renomear a rede**, em **Desejo**.

3 Digite o nome da rede na caixa **Renomear rede**.

4 Clique em **OK**.

Observação: O link **Renomear rede** só está disponível quando não há itens selecionados no mapa de rede. Para desmarcar um item, clique no item selecionado ou clique em uma área em branco no mapa de rede.

Mostrar ou ocultar itens do mapa de rede

Por padrão, todos os computadores e componentes da sua rede doméstica são exibidos no mapa de rede. Contudo, se você tiver ocultado itens, é possível exibi-los novamente a qualquer momento. Somente os itens não gerenciados podem ser ocultados; não é possível ocultar os computadores gerenciados.

Para...	No menu Básico ou Avançado, clique em **Gerenciar rede** e, em seguida realize este procedimento...
Ocultar um item no mapa de rede	Clique em um item do mapa de rede e clique em **Ocultar este item** em **Desejo**. Na caixa de diálogo de confirmação, clique em **Sim**.
Mostrar itens ocultos no mapa de rede	Em **Desejo**, clique em **Mostrar itens ocultos**.

Exibir detalhes do item

Você pode exibir as informações detalhadas de qualquer componente da sua rede, selecionando-o no mapa de rede. Essas informações incluem o nome do componente, seu status de proteção e outros dados necessários para gerenciá-lo.

Para exibir os detalhes de um item:

1. Clique no ícone de um item no mapa de rede.
2. Em **Detalhes**, exiba as informações sobre o item.

Associando à rede gerenciada

Para que um computador possa ser gerenciado remotamente ou receber permissão para gerenciar outros computadores remotamente, ele deve se tornar um membro confiável da rede. A associação à rede é concedida para novos computadores por membros existentes da rede (computadores) com permissões administrativas. Para garantir que apenas computadores confiáveis se associem à rede, os usuários do computador que concede a permissão e do computador que está se associando a ela devem autenticar um ao outro.

Quando um computador se associa à rede, ele é solicitado a mostrar o seu status de proteção do McAfee para outros computadores da rede. Se um computador concordar em mostrar seu status de proteção, ele se tornará um membro *gerenciado* da rede. Se um computador se recusar a mostrar seu status de proteção, ele se tornará um membro *não gerenciado* da rede. Os membros não gerenciados da rede geralmente são computadores convidados que desejam acesso a outros recursos de rede (como, por exemplo, compartilhamento de arquivos ou da impressora).

Observação: Depois da associação, se você tiver outros programas de rede da McAfee instalados (o McAfee Wireless Network Security ou o EasyNetwork, por exemplo), o computador também será reconhecido como membro gerenciado nesses programas. O nível de permissão atribuído a um computador no Network Manager aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o que significam permissões de convidado, total ou administrativa em outros programas de rede da McAfee, consulte a documentação fornecida com o programa.

Associar-se a uma rede gerenciada

Quando receber um convite para se associar a uma rede gerenciada, você poderá aceitar ou rejeitar o convite. Também é possível determinar se deseja que este computador e os outros computadores da rede monitorem as configurações de segurança uns dos outros (se os serviços de proteção contra vírus estão atualizados ou não, por exemplo).

Para associar-se a uma rede gerenciada:

1. Na caixa de diálogo de convite, marque a caixa de seleção **Permitir que este computador e outros computadores monitorem as configurações de segurança uns dos outros** para permitir que outros computadores da rede gerenciada monitorem as configurações de segurança do seu computador.
2. Clique em **Associar-se**.
   Quando você aceitar o convite, duas cartas de baralho serão exibidas.
3. Confirme se as cartas de baralho são as mesmas exibidas no computador que o convidou para se associar à rede gerenciada.
4. Clique em **Confirmar**.

Observação: Se o computador que o convidou não exibir as mesmas cartas que estão sendo exibidas na caixa de diálogo de confirmação de segurança, isso significa que houve uma violação de segurança na rede gerenciada. Associar-se à rede poderia colocar seu computador em risco, portanto, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Convidar um computador para associar-se à rede gerenciada

Se um computador for adicionado ou outro computador não gerenciado estiver presente na rede, você poderá convidá-lo a se associar à rede gerenciada. Apenas os computadores com permissões administrativas na rede podem convidar outros computadores. Ao enviar um convite, você também poderá especificar o nível de permissão que deseja atribuir ao computador que irá se associar.

Para convidar um computador para associar-se à rede gerenciada:

1. Clique no ícone de um computador não gerenciado no mapa de rede.
2. Clique em **Monitorar este computador**, em **Desejo.**
3. Na caixa de diálogo Convidar um computador para associar-se a esta rede gerenciada, clique em uma destas opções:
   - **Conceder acesso convidado**
     O acesso de convidado permite que o computador acesse a rede.
   - **Conceder acesso total para todos os aplicativos da rede gerenciada**
     O acesso total (como o acesso de convidado) permite que o computador acesse a rede.
   - **Conceder acesso administrativo para todos os aplicativos da rede gerenciada**
     O acesso administrativo permite que o computador acesse a rede com permissões administrativas. Ele também permite que o computador conceda acesso a outros computadores que queiram se associar à rede gerenciada.

4 Clique em **Convidar**.
Um convite para se associar à rede gerenciada é enviado para o computador. Quando o computador aceitar o convite, duas cartas de baralho são exibidas.

5 Confirme se as cartas de baralho são as mesmas exibidas no computador que você convidou para se associar à rede gerenciada.

6 Clique em **Conceder acesso**.

Observação: Se o computador que você convidou não exibir as mesmas cartas que estão sendo exibidas na caixa de diálogo de confirmação de segurança, isso significa que houve uma violação de segurança na rede gerenciada. Permitir que o computador tenha acesso à rede pode colocar outros computadores em risco, portanto, clique em **Rejeitar acesso** na caixa de diálogo de confirmação de segurança.

Parar de confiar nos computadores da rede

Caso tenha concordado em confiar em outros computadores por engano, você pode parar de confiar neles.

Para parar de confiar nos computadores da rede:

- Clique em **Parar de confiar nos computadores desta rede** em **Desejo**.

Observação: O link **Parar de confiar nos computadores desta rede** só estará disponível quando nenhum outro computador gerenciado tiver se associado à rede.

CAPÍTULO 12

Gerenciando a rede remotamente

Depois de configurar sua rede gerenciada, você pode usar o Network Manager para gerenciar remotamente os computadores e componentes que fazem parte da rede. É possível gerenciar o status e os níveis de permissão dos computadores e componentes e corrigir vulnerabilidades da segurança remotamente.

Neste capítulo

Monitorando status e permissões

Uma rede gerenciada possui dois tipos de membros: membros gerenciados e não gerenciados. Membros gerenciados permitem que outros computadores da rede monitores seu status de proteção McAfee, enquanto membros não gerenciados não o permitem. Os membros não gerenciados geralmente são computadores convidados que desejam acessar outros recursos da rede (como, por exemplo, compartilhamento de arquivos ou de impressora). Um computador não gerenciado pode ser convidado a se tornar gerenciado a qualquer momento por outro computador da rede. Da mesma forma, um computador danificado pode se tornar não gerenciado a qualquer momento.

Os computadores gerenciados possuem uma permissão administrativa, total ou de convidado. As permissões administrativas permitem que o computador gerenciado gerencie o status de proteção de todos os computadores gerenciados na rede e que conceda acesso à rede para outros computadores. As permissões total e de convidado permitem somente que um computador acesse a rede. Você pode modificar o nível de permissão de um computador a qualquer momento.

Como uma rede gerenciada também é composta por dispositivos (como roteadores, por exemplo), você poderá usar o Network Manager para gerenciá-los. Também é possível configurar e modificar as propriedades de exibição do dispositivo no mapa de rede.

Monitorar o status de proteção de um computador

Se o status de proteção de um computador não estiver sendo monitorado na rede (porque o computador não é um membro da rede ou não é gerenciado), você pode fazer uma solicitação para monitorá-lo.

Para monitorar o status de proteção de um computador:

1 Clique no ícone de um computador não gerenciado no mapa de rede.

2 Clique em **Monitorar este computador**, em **Desejo**.

Parar de monitorar o status de proteção de um computador

Você pode parar de monitorar o status de proteção de um computador gerenciado em sua rede particular. A partir desse momento o computador não será mais gerenciado.

Para parar de monitorar o status de proteção de um computador:

1. Clique no ícone de um computador gerenciado no mapa de rede.
2. Clique em **Parar de monitorar este computador**, em **Desejo**.
3. Na caixa de diálogo de confirmação, clique em **Sim**.

Modificar as permissões de um computador gerenciado

Você pode modificar as permissões de um computador gerenciado a qualquer momento. Isso permite que você ajuste os computadores que poderão monitorar os status de proteção (configurações de segurança) de outros computadores da rede.

Para modificar as permissões de um computador gerenciado:

1. Clique no ícone de um computador gerenciado no mapa de rede.
2. Clique em **Monitorar permissões para este computador**, em **Desejo**.
3. Na caixa de diálogo de modificação das permissões, marque ou desmarque a caixa de seleção que determina se este e outros computadores da rede gerenciada poderão monitorar o status de proteção uns dos outros.
4. Clique em **OK**.

Gerenciar um dispositivo

Você pode gerenciar um dispositivo acessando a sua página administrativa da Web a partir do Network Manager.

Para gerenciar um dispositivo:

1. Clique no ícone de um dispositivo no mapa de rede.
2. Clique em **Gerenciar este dispositivo**, em **Desejo**.
   Um navegador da Web é aberto e exibe a página administrativa do dispositivo na Web.
3. No navegador da Web, insira as suas informações de logon e defina as configurações de segurança do dispositivo.

Observação: Se o dispositivo for um ponto de acesso ou um roteador sem fio protegido pelo Wireless Network Security, você terá que usar o Wireless Network Security para definir as configurações de segurança do dispositivo.

Modificar as propriedades de exibição de um dispositivo

Ao modificar as propriedades de exibição de um dispositivo, você poderá alterar o nome de exibição do dispositivo no mapa da rede e especificar se ele é um roteador sem fio.

Para modificar as propriedades de exibição de um dispositivo:

1. Clique no ícone de um dispositivo no mapa de rede.
2. Clique em **Modificar propriedades de dispositivo**, em **Desejo**.
3. Para especificar o nome de exibição do dispositivo, digite um nome na caixa **Nome**.
4. Para especificar o tipo de dispositivo, clique em uma das seguintes opções:
   - **Roteador**
     Representa um roteador doméstico padrão.
   - **Roteador sem fio**
     Representa um roteador doméstico sem fio.
5. Clique em **OK**.

Corrigindo vulnerabilidades de segurança

Computadores gerenciados com permissões administrativas podem monitorar o status de proteção McAfee de outros computadores gerenciados na rede e corrigir remotamente quaisquer problemas de vulnerabilidade de segurança reportados. Por exemplo, se o status de proteção McAfee de um computador indicar que o VirusScan está desativado, outro computador gerenciado com permissões administrativas poderá *corrigir* essa vulnerabilidade de segurança, ativando o VirusScan remotamente.

Quando vulnerabilidades de segurança são corrigidas remotamente, o Network Manager automaticamente repara a maioria dos problemas reportados. No entanto, algumas vulnerabilidades podem exigir intervenção manual no computador local. Nesse caso, o Network Manager corrige os problemas que podem ser reparados remotamente e solicita que você corrija os problemas restantes efetuando login no SecurityCenter no computador vulnerável e seguindo as recomendações fornecidas. Em alguns casos, a correção sugerida é a instalação do software de segurança McAfee 2007 nos computadores remotos da rede.

Corrigir vulnerabilidades de segurança

Você pode usar o Network Manager para corrigir automaticamente a maioria das vulnerabilidades de segurança em computadores gerenciados remotos. Por exemplo, se o VirusScan estiver desativado em um computador remoto, você poderá usar o Network Manager para ativá-lo automaticamente.

Para corrigir vulnerabilidades de segurança:

1. Clique no ícone de um item no mapa de rede.
2. Exiba o status de proteção do item, em **Detalhes**.
3. Clique em **Corrigir vulnerabilidades de segurança**, em **Desejo**.
4. Depois de corrigir os problemas de segurança, clique em **OK**.

Observação: Apesar de o Network Manager corrigir automaticamente a maioria das vulnerabilidades de segurança, para efetuar alguns reparos pode ser necessário iniciar o SecurityCenter no computador vulnerável e seguir as recomendações fornecidas.

Instalar software de segurança McAfee em computadores remotos

Se um ou mais computadores de sua rede não estiverem executando software de segurança McAfee, o status de segurança deles não poderá ser monitorado remotamente. Se desejar monitorar esses computadores remotamente, você deverá ir até cada um deles e instalar o software de segurança McAfee.

Para instalar software de segurança McAfee em computadores remotos:

1 Em um navegador no computador remoto, vá para http://download.mcafee.com/us/.

2 Siga as instruções na tela para instalar o software de segurança Mcafee no computador.

CAPÍTULO 13

McAfee VirusScan

O VirusScan oferece proteção abrangente, confiável e atualizada contra vírus e spyware. Equipado com a premiada tecnologia de varredura da McAfee, o VirusScan protege o computador contra vírus, worms, cavalos de Tróia, scripts suspeitos, rootkits, sobrecargas de buffer, ataques híbridos, spyware, programas potencialmente indesejados e outras ameaças.

Neste capítulo

Recursos

Essa versão do VirusScan oferece os seguintes recursos.

Proteção contra vírus

A varredura em tempo real varre os arquivos quando eles são acessados por você ou pelo seu computador.

Varredura

Procura por vírus e outras ameaças em unidades de disco rígido, em disquetes e em arquivos e pastas individuais. Você também pode clicar com o botão direito do mouse em um item para examiná-lo.

Detecção de spyware e adware

O VirusScan identifica e remove spyware, adware e outros programas que podem comprometer a sua privacidade e reduzir o desempenho do seu computador.

Atualizações automáticas

As atualizações automáticas protegem contra as mais recentes ameaças ao computador, identificadas ou não.

Varredura rápida em segundo plano

As varreduras rápidas e discretas identificam e destroem vírus, cavalos de Tróia, worms, spyware, adware, discadores e outras ameaças sem interromper o seu trabalho.

Alertas de segurança em tempo real

Os alertas de segurança notificam emergências de epidemias de vírus e ameaças à segurança. Também oferecem opções de resposta para remover, neutralizar ou saber mais sobre a ameaça.

Detecção e limpeza em vários pontos de entrada

O VirusScan monitora e limpa os principais pontos de entrada do seu computador: e-mails, anexos de mensagens instantâneas e downloads da Internet.

Monitoração de e-mail para atividades semelhantes às de worms

O WormStopper™ impede que os cavalos de Tróia enviem worms por e-mail para outros computadores e avisa antes que programas de e-mails desconhecidos enviem mensagens de e-mail a outros computadores.

Monitoração de script para atividades semelhantes a de worms

O ScriptStopper™ bloqueia a execução de scripts conhecidos mal-intencionados no seu computador.

McAfee X-ray for Windows

O McAfee X-ray detecta e elimina rootkits e outros programas que se ocultam no Windows.

Proteção contra a sobrecarga do buffer

A proteção contra a sobrecarga do buffer protege contra sobrecargas de buffer. Sobrecargas de buffer ocorrem quando programas ou processos suspeitos tentam armazenar dados em um buffer (área de armazenagem temporária de dados) além de seu limite, corrompendo ou sobrescrevendo dados válidos em buffers adjacentes.

McAfee SystemGuards

Os SystemGuards examinam o computador em busca de comportamentos específicos que possam indicar atividade de vírus, spyware ou hackers.

CAPÍTULO 14

Gerenciando a proteção contra vírus

Você pode gerenciar em tempo real a proteção de SystemGuard e a proteção contra vírus, spyware e script. Por exemplo, você pode desativar a varredura ou especificar o que deve ser submetido a ela.

Apenas usuários com direitos de Administrador podem modificar opções avançadas.

Neste capítulo

Usando a proteção contra vírus

Quando a proteção contra vírus (varredura em tempo real) é iniciada, ela monitora constantemente o computador em busca de atividades de vírus. A varredura em tempo real varre os arquivos sempre que são acessados por você ou seu computador. Quando a proteção contra vírus detecta um arquivo infectado, ela tenta limpar ou remover a infecção. Se um arquivo não puder ser limpo ou removido, um alerta o avisará para que tome outras providências.

Tópicos relacionados

- Noções básicas sobre os alertas de segurança (página 107)

Desativar proteção contra vírus

Se você desativar a proteção contra vírus, seu computador não será monitorado continuamente quanto às atividades de vírus. Se você precisar interromper a proteção contra vírus, certifique-se de não estar conectado à Internet.

Observação: Ao desativar a proteção contra vírus você também desativa a proteção em tempo real contra spyware, bem como a proteção para e-mail e mensagens instantâneas.

Para desativar a proteção contra vírus:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador e arquivos**.
3. Em **Proteção contra vírus**, clique em **Desligado**.
4. Na caixa de diálogo de confirmação, execute uma das seguintes ações:
   - Para reiniciar a proteção contra vírus após um período especificado, selecione a caixa de seleção **Reativar varredura em tempo real depois de** e selecione um prazo no menu.
   - Para que a proteção contra vírus não seja reiniciada após um período específico, desmarque a caixa de seleção **Reativar proteção contra vírus depois de**.
5. Clique em **OK**.

Se a proteção em tempo real estiver configurada para iniciar quando o Windows for iniciado, seu computador estará protegido quando for reiniciado.

Tópicos relacionados

- Configurar proteção em tempo real (página 78)

Ativar proteção contra vírus

A proteção contra vírus monitora continuamente o seu computador em busca de atividade de vírus.

Para ativar a proteção contra vírus:

1 No menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador e arquivos**.

3 Em **Proteção contra vírus**, clique em **Ligado**.

Configurando proteção em tempo real

Você pode modificar a proteção contra vírus em tempo real. Por exemplo, você pode varrer apenas os arquivos de programa e os documentos, ou desativar a varredura em tempo real quando Windows for iniciado (não recomendado).

Configurar proteção em tempo real

Você pode modificar a proteção contra vírus em tempo real. Por exemplo, você pode varrer apenas os arquivos de programa e os documentos, ou desativar a varredura em tempo real quando Windows for iniciado (não recomendado).

Para configurar a proteção em tempo real:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador e arquivos**.

3 Em **Proteção contra vírus**, clique em **Avançado**.

4 Selecione ou limpe as seguintes caixas de seleção:

- **Fazer varredura para vírus desconhecidos usando heurística**: É feita uma correspondência entre arquivos e assinaturas de vírus conhecidos para detectar sinais de vírus não identificados. Essa opção proporciona a varredura mais completa, mas geralmente é mais lenta do que a varredura normal.
- **Fazer varredura na unidade de disquete ao desligar**: Quando o computador é encerrado, ocorre a varredura da unidade de disquete.
- **Fazer a varredura para spyware e programas potencialmente indesejados**: São detectados e removidos spywares, adwares e outros programas com potencial de coletar e transmitir dados sem a sua permissão.
- **Fazer varredura e remover cookies de rastreamento**: São detectados e removidos os cookies com potencial de coletar e transmitir dados sem a sua permissão. Um cookie identifica os usuários quando eles visitam uma página da Web.
- **Fazer varredura de unidades de rede**: É feita uma varredura nas unidades conectadas à sua rede.
- **Ativar proteção contra a sobrecarga do buffer**: Se a atividade de sobrecarga de buffer for detectada, ela será bloqueada e você será alertado.
- **Iniciar varredura em tempo real quando o Windows for iniciado (recomendável)**: A proteção em tempo real será ativada sempre que você iniciar o seu computador, mesmo se ela tiver sido desativada em uma sessão.

5 Clique em um dos seguintes botões:

- **Todos os arquivos (recomendável)**: É feita uma varredura em cada tipo de arquivo usado em seu computador. Use essa opção para obter a varredura mais completa.
- **Apenas arquivos de programa e documentos**: É feita uma varredura apenas nos arquivos de programa e nos documentos.

6 Clique em **OK**.

Usando a proteção contra spyware

A proteção contra spyware remove spywares, adwares e outros programas potencialmente indesejados que coletam e transmitem dados sem a sua permissão.

Desativar proteção contra spyware

Se você desativar a proteção contra spyware, os programas potencialmente indesejados que coletam e transmitem dados sem a sua permissão não serão detectados.

Para desativar a proteção contra spyware:

1 No menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador e arquivos**.

3 Em **Proteção contra spyware**, clique em **Desligado**.

Ativar proteção contra spyware

A proteção contra spyware remove spywares, adwares e outros programas potencialmente indesejados que coletam e transmitem dados sem a sua permissão.

Para ativar a proteção contra spyware:

1 No menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador e arquivos**.

3 Em **Proteção contra spyware**, clique em **Ligado**.

Usando SystemGuards

Os SystemGuards detectam alterações potencialmente não autorizadas em seu computador e alertam quando elas ocorrem. Você pode rever essas alterações e decidir se devem ser permitidas.

Os SystemGuards são categorizados da seguinte maneira.

Programa

Os SystemGuards de programas detectam alterações em seus arquivos de inicialização, extensões e arquivos de configuração.

Windows

Os SystemGuards do Windows detectam alterações nas configurações do Internet Explorer, incluindo atributos do navegador e configurações de segurança.

Navegador

Os SystemGuards do navegador detectam alterações nos serviços, certificados e arquivos de configuração do Windows ɜ.

Desativar SystemGuards

Se você desativar os SystemGuards, as alterações potencialmente não autorizadas no computador não serão detectadas.

Para desativar todos os SystemGuards:

1 No menu Avançado, clique em **Configurar**.
2 No painel Configurar, clique em **Computador e arquivos**.
3 Em **Proteção de SystemGuard**, clique em **Desligado**.

Ativar SystemGuards

Os SystemGuards detectam alterações potencialmente não autorizadas em seu computador e alertam quando elas ocorrem.

Para ativar os SystemGuards:

1 No menu Avançado, clique em **Configurar**.
2 No painel Configurar, clique em **Computador e arquivos**.
3 Em **Proteção de SystemGuard**, clique em **Ligado**.

Configurando os SystemGuards

Você pode modificar os SystemGuards. Para cada alteração detectada, você pode decidir se deseja ser alertado e registrar o evento, apenas registrar o evento ou desativar o SystemGuard.

Configurar SystemGuards

Você pode modificar os SystemGuards. Para cada alteração detectada, você pode decidir se deseja ser alertado e registrar o evento, apenas registrar o evento ou desativar o SystemGuard.

Para configurar os SystemGuards:

1. No menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador e arquivos**.
3. Em **Proteção de SystemGuard**, clique em **Avançado**.
4. Na lista SystemGuards, clique em uma categoria para exibir a lista de SystemGuards associados e os respectivos status.
5. Clique no nome de um SystemGuard.
6. Em **Detalhes**, exiba as informações sobre o SystemGuard.
7. Em **Desejo**, execute uma das seguintes ações:
   - Clique em **Mostrar alertas**, se você deseja ser alertado quando ocorrer uma alteração e o evento for registrado.
   - Clique em **Registrar apenas as alterações**, se você não deseja que uma medida seja tomada quando uma alteração for detectada. A alteração é apenas registrada.
   - Clique em **Desativar este SystemGuard** para desligar o SystemGuard. Você não será alertado quando ocorrer uma alteração e o evento não for registrado.
8. Clique em **OK**.

Noções básicas sobre os SystemGuards

Os SystemGuards detectam alterações potencialmente não autorizadas em seu computador e alertam quando elas ocorrem. Você pode rever essas alterações e decidir se devem ser permitidas.

Os SystemGuards são categorizados da seguinte maneira.

Programa

Os SystemGuards de programas detectam alterações em seus arquivos de inicialização, extensões e arquivos de configuração.

Windows

Os SystemGuards do Windows detectam alterações nas configurações do Internet Explorer, incluindo atributos do navegador e configurações de segurança.

Navegador

Os SystemGuards do navegador detectam alterações nos serviços, certificados e arquivos de configuração do Windows ᴲ.

Sobre os SystemGuards de programas

Os SystemGuards de programas detectam os seguintes itens.

Instalações de ActiveX

Detecte os programas ActiveX transferidos por download através do Internet Explorer. Os programas ActiveX são transferidos por download a partir de sites e armazenados em seu computador em C:\Windows\Downloaded Program Files ou C:\Windows\Temp\Temporary Internet Files. Também são feitas referências a eles no Registro por meio de seus CLSID (longa seqüência de números entre as chaves).

O Internet Explorer utiliza vários programas ActiveX legítimos. Se você não tem certeza sobre um programa ActiveX, poderá excluí-lo sem danificar o computador. Se esse programa for necessário posteriormente, o Internet Explorer fará seu download automaticamente na próxima vez em que você retornar a um site na Web que exija o programa.

Itens de inicialização

Monitore alterações realizadas em suas pastas e chaves de Registro de inicialização. As chaves de Registro de inicialização nas pastas de inicialização e Registro do Windows no menu Iniciar armazenam os caminhos dos programas em seu computador. Os programas listados nesses locais são carregados quando o Windows é iniciado. Spywares ou outros programas potencialmente indesejados geralmente tentam ser carregados quando o Windows é iniciado.

Ganchos de execução de shell do Windows

Monitore alterações feitas à lista de programas carregados no explorer.exe. Um gancho de execução de shell é um programa que é carregado dentro do shell do Windows do explorer.exe. Um programa de gancho de execução de shell recebe todos os comandos de execução de um computador. Qualquer programa carregado no shell do explorer.exe pode executar uma tarefa adicional antes que outro programa seja efetivamente iniciado. Spywares ou outros programas potencialmente indesejados podem usar ganchos de execução de shell para impedir a execução de programas de segurança.

Carregamento de atraso do objeto de serviço do Shell

Monitore as alterações nos arquivos relacionados no Carregamento de atraso do objeto de serviço do Shell. Esses arquivos são carregados pelo explorer.exe quando o computador é iniciado. Como o explore.exe é o shell do seu computador, ele sempre é iniciado, carregando os arquivos sob essa chave. Esses arquivos são carregados no começo do processo de inicialização antes de qualquer intervenção humana.

Sobre os SystemGuards do Windows

Os SystemGuards do Windows detectam os seguintes itens.

Identificadores do menu contextual

Impeça alterações não autorizadas aos menus de contexto do Windows. Esses menus permitem que você clique com o botão direito do mouse em um arquivo e execute ações específicas relevantes para esse arquivo.

DLLs do AppInit

Impeça alterações ou adições não autorizadas nos arquivos AppInit.DLLs do Windows. O valor do registro AppInit_DLLs contém uma lista de arquivos que são carregados quando um user32.dll é carregada. Os arquivos no valor AppInit_DLLs são carregados no início da rotina de inicialização do Windows, permitindo que um .DLL potencialmente nocivo se oculte antes que ocorra qualquer intervenção humana.

Arquivo Hosts do Windows

Monitore as alterações no arquivo Hosts do seu computador. Seu arquivo Hosts é usado para redirecionar determinados nomes de domínio para endereços IP específicos. Por exemplo, quando você visita www.exemplo.com.br, seu navegador verifica o arquivo Hosts, vê uma entrada para exemplo.com.br e indica o endereço IP para esse domínio. Alguns programas spyware tentam mudar seu arquivo Hosts para redirecionar seu navegador para outro site ou impedir seu software de ser corretamente atualizado.

Shell Winlogon

Monitore o Shell Winlogon. Esse shell é carregado quando um usuário efetua logon no Windows. O shell é a principal Interface de usuário usada para gerenciar o Windows e normalmente é o Windows Explorer (explore.exe). No entanto, o shell do Windows pode ser facilmente modificado para indicar outro programa. Se isso ocorrer, outro programa que não o shell do Windows será iniciado sempre que um usuário efetuar logon.

Inicialização de usuário Winlogon

Monitore as alterações em suas configurações de logon de usuário no Windows. A chave HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit especifica que programa é iniciado depois que um usuário efetua logon no Windows. O programa padrão restaura perfil, fontes, cores e outras configurações do seu nome de usuário. Spywares e outros programas potencialmente indesejados podem tentar ser iniciados, adicionando-se a essa chave.

Protocolos do Windows

Monitore as alterações em seus protocolos de rede. Alguns spywares e outros programas potencialmente indesejados assumem controle de certos caminhos pelos quais o computador envia e recebe informações. Isso é realizado através dos filtros e manipuladores de protocolo do Windows.

Provedores de serviços em camadas Winsock

Monitore os provedores de serviços em camadas (LSP), que podem interceptar os seus dados na rede e alterá-los ou redirecioná-los. LSPs legítimos incluem softwares de controles pelos pais, firewalls e outros programas de segurança. Spywares podem usar LSPs para monitorar suas atividades na Internet e modificar seus dados. Para evitar a reinstalação do sistema operacional, use programas da McAfee para remover automaticamente spywares e LSPs comprometidos.

Comandos abertos do Shell do Windows

Impeça alterações nos Comandos abertos do Shell do Windows (explorer.exe). Comandos abertos do shell permitem que um programa específico seja executado sempre que um certo tipo de arquivo for executado. Por exemplo, um worm pode tentar ser executado sempre que um aplicativo .exe for executado.

Programador de tarefas compartilhadas

Monitore a chave de registro SharedTaskScheduler, que contém uma lista de programas que são executados quando o Windows é iniciado. Alguns spywares ou outros programas potencialmente indesejados modificam essa chave e adicionam-se à lista sem a sua permissão.

Serviço do Windows Messenger

Monitore o serviço do Windows Messenger, um recurso não documentado do Windows Messenger que permite aos usuários enviar mensagens pop-up. Alguns spywares e outros programas potencialmente indesejados tentam ativar o serviço e enviar anúncios não solicitados. O serviço também pode ser explorado através de uma vulnerabilidade conhecida, para executar o código remotamente.

Arquivo Win.ini do Windows

O arquivo win.ini é baseado em texto e fornece uma lista de programas que serão executados quando o Windows for iniciado. A sintaxe para carregar esses programas está no arquivo usado para suportar versões mais antigas do Windows. A maioria dos programas não usa o arquivo sin.ini para carregar programas. Porém, alguns spywares ou outros programas potencialmente indesejados são desenvolvidos para tirar proveito dessa sintaxe e serem carregados durante a inicialização do Windows.

Sobre os SystemGuards do navegador

Os SystemGuards do navegador detectam os seguintes itens.

Objetos auxiliares do navegador

Monitore os acréscimos aos Objetos auxiliares do navegador (BHOs). Os BHOs são programas que agem como plug-ins do Internet Explorer. Spywares e seqüestradores de navegador geralmente usam BHOs para mostrar anúncios ou rastrear hábitos de navegação. Os BHOs também são usados por muitos programas legítimos, como barras de ferramentas de pesquisa.

Barras do Internet Explorer

Monitore as alterações feitas na lista de programas da barra do Internet Explorer. Uma barra do Explorer é um painel, como os painéis de Busca, Favoritos ou Histórico, que você encontra no Internet Explorer (IE) ou no Windows Explorer.

Plug-ins do Internet Explorer

Impeça que o spyware instale plug-ins do Internet Explorer. Os plug-ins do Internet Explorer são as extensões de software carregadas quando o Internet Explorer é iniciado. O spyware geralmente utiliza os plug-ins do Internet Explorer para mostrar anúncios ou rastrear hábitos de navegação. Os plug-ins legítimos agregam funcionalidade ao Internet Explorer.

ShellBrowser do Internet Explorer

Monitore as alterações feitas na instância do ShellBrowser do Internet Explorer. O ShellBrowser do Internet Explorer contém informações e configurações sobre uma instância do Internet Explorer. Se essas configurações forem alteradas ou um novo ShellBrowser for instalado, esse ShellBrowser poderá assumir controle total do Internet Explorer, adicionando recursos como barras de ferramentas, menus e botões.

WebBrowser do Internet Explorer

Monitore as alterações feitas na instância do WebBrowser do Internet Explorer. O WebBrowser do Internet Explorer contém informações e configurações sobre uma instância do Internet Explorer. Se essas configurações forem alteradas ou um novo WebBrowser for instalado, esse WebBrowser poderá assumir controle total do Internet Explorer, adicionando recursos como barras de ferramentas, menus e botões.

Ganchos de pesquisa de URL do Internet Explorer

Monitore as alterações feita nos ganchos de pesquisa de URL do Internet Explorer. Um Gancho de pesquisa de URL é usado quando você digita um endereço no campo de localização do navegador sem um protocolo, como http:// ou ftp:// no endereço. Quando você digita um endereço assim, o navegador pode usar o UrlSearchHook para pesquisar na Internet e encontrar o local que você digitou.

URLs do Internet Explorer

Monitore as alterações nas URLs predefinidas do Internet Explorer. Isso evita que spywares ou programas potencialmente indesejáveis alterem as configurações do seu navegador sem a sua permissão.

Restrições do Internet Explorer

Monitore as restrições do Internet Explorer, que permitem que um administrador do computador impeça que um usuário altere a página inicial ou outras opções no Internet Explorer. Essas opções aparecem apenas se seu administrador defini-las intencionalmente.

Zonas de segurança do Internet Explorer

Monitore as zonas de segurança do Internet Explorer. O Internet Explorer possui quatro zonas de segurança predefinidas: Internet, Intranet local, Sites confiáveis e Sites restritos. Cada uma dessas zonas tem sua própria configuração de segurança, que é predefinida ou personalizada. As zonas de segurança são alvos de alguns spywares ou outros programas potencialmente indesejados, porque a redução no nível de segurança permite que esses programas enganem os alertas de segurança e ajam sem ser detectados.

Sites confiáveis do Internet Explorer

Monitore os sites confiáveis do Internet Explorer. A lista de sites confiáveis é um diretório dos sites da Web em que você confia. Alguns spywares ou outros programas potencialmente indesejados têm esta lista como alvo porque ela fornece um método para confiar em sites suspeitos sem a sua permissão.

Política do Internet Explorer

Monitore as políticas do Internet Explorer. Essas configurações de políticas normalmente são alteradas por administradores do sistema, mas podem ser exploradas por spywares. As alterações podem evitar que você defina uma nova página inicial ou podem ocultar a exibição de guias na caixa de diálogo Opções da Internet no menu Ferramentas.

Usando a varredura de scripts

Um script pode criar, copiar ou excluir os arquivos. Ele também pode abrir o Registro do Windows.

A varredura de scripts bloqueia automaticamente a execução de scripts mal-intencionados conhecidos no seu computador.

Desativar varredura de scripts

Se você desativar a varredura de scripts, as execuções de scripts suspeitos não serão detectadas.

Para desativar a varredura de scripts:

1. No menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador e arquivos**.
3. Em **Proteção de varredura de scripts**, clique em **Desligado**.

Ativar a varredura para scripts

A varredura de scripts irá alertá-lo se uma execução de script resultar na criação, na cópia ou na exclusão de arquivos, ou na abertura do Registro do Windows.

Para ativar a varredura de scripts:

1. No menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador e arquivos**.
3. Em **Proteção de varredura de scripts**, clique em **Ligado**.

Usando a proteção de e-mail

A proteção de e-mail detecta e bloqueia as ameaças nas mensagens de e-mail recebidas (POP3) e enviadas (SMTP) e nos anexos, que incluem vírus, cavalos de Tróia, worms, spywares, adwares e outras ameaças.

Desativar a proteção de e-mail

Se você desativar a proteção de e-mail, as ameaças potenciais nas mensagens de e-mail recebidas (POP3) e enviadas (SMTP) e nos anexos não serão detectadas.

Para desativar a proteção de e-mail:

1 No menu Avançado, clique em **Configurar**.
2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3 Em **Proteção de e-mail**, clique em **Desligado**.

Ativar a proteção de e-mail

A proteção de e-mail detecta as ameaças nas mensagens de e-mail recebidas (POP3) e enviadas (SMTP) e nos anexos.

Para ativar a proteção de e-mail:

1 No menu Avançado, clique em **Configurar**.
2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3 Em **Proteção de e-mail**, clique em **Ligado**.

Configurando a proteção de e-mail

As opções de proteção de mensagem de e-mail permitem que você faça varredura nas mensagens de e-mail recebidas, mensagens de e-mail enviadas e worms. Os worms replicam e consomem recursos do sistema, reduzindo o desempenho ou interrompendo as tarefas. Os worms podem enviar cópias de si mesmos através de mensagens de e-mail. Por exemplo, eles podem tentar enviar mensagens de e-mail para as pessoas em sua lista de endereços.

Configurar a proteção de e-mail

As opções de proteção de mensagem de e-mail permitem que você faça varredura nas mensagens de e-mail recebidas, mensagens de e-mail enviadas e worms.

Para configurar a proteção de e-mail:

1. No menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção de e-mail**, clique em **Avançado**.
4. Selecione ou limpe as seguintes caixas de seleção:
   - **Fazer varredura de mensagens de e-mail recebidas**: As mensagens recebidas (POP3) são examinadas em busca de ameaças em potencial.
   - **Fazer varredura de mensagens de e-mail enviadas**: As mensagens enviadas (SMTP) são examinadas em busca de ameaças em potencial.
   - **Ativar o WormStopper**: O WormStopper bloqueia worms nas mensagens de e-mail.
5. Clique em **OK**.

Usando a proteção para mensagens instantâneas

A proteção para mensagens instantâneas detecta as ameaças nos anexos das mensagens instantâneas recebidas.

Desativar a proteção para mensagens instantâneas

Se você desativar a proteção para mensagens instantâneas, as ameaças nos anexos das mensagens instantâneas recebidas não serão detectadas.

Para desativar a proteção para mensagens instantâneas:

1 No menu Avançado, clique em **Configurar**.
2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3 Em **Proteção para mensagens instantâneas**, clique em **Desligado**.

Ativar a proteção para mensagens instantâneas

A proteção para mensagens instantâneas detecta as ameaças nos anexos das mensagens instantâneas recebidas.

Para ativar a proteção para mensagens instantâneas:

1 No menu Avançado, clique em **Configurar**.
2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3 Em **Proteção para mensagens instantâneas**, clique em **Ligado**.

CAPÍTULO 15

Fazendo a varredura manual do computador

É possível procurar por vírus e outras ameaças em unidades de disco rígido, disquetes e em arquivos e pastas individuais. Quando o VirusScan encontra um arquivo suspeito, ele tenta limpá-lo, a menos que seja um programa potencialmente indesejado. Se o VirusScan não conseguir limpar o arquivo, você poderá colocar o arquivo em quarentena ou excluí-lo.

Neste capítulo

Varredura manual

Você pode fazer a varredura manualmente a qualquer momento. Por exemplo, se você acabou de instalar o VirusScan, poderá executar uma varredura para garantir que o computador não possui nenhum vírus ou outras ameaças. Ou, se você desativou a varredura em tempo real, poderá executar uma varredura para garantir que o computador ainda esteja seguro.

Varredura usando as configurações de varredura manual

Esse tipo de varredura usa as configurações de varredura manual que você especifica. O VirusScan examina o interior dos arquivos compactados (.zip, .cab, etc.), mas conta um arquivo compactado como um arquivo. Além disso, o número de arquivos examinados pode variar se você tiver excluído os arquivos temporários da Internet após a última varredura.

Para examinar usando as configurações de varredura manual:

1. No Menu básico, clique em **Varredura**. Quando a varredura for concluída, um resumo mostrará o número de itens examinados e detectados, o número de itens limpos e quando ocorreu a última varredura.
2. Clique em **Concluir**.

Tópicos relacionados

- Configurando varreduras manuais (página 98)

Varredura sem usar as configurações de varredura manual

Esse tipo de varredura não usa as configurações de varredura manual que você especifica. O VirusScan examina o interior dos arquivos compactados (.zip, .cab, etc.), mas conta um arquivo compactado como um arquivo. Além disso, o número de arquivos examinados pode variar se você tiver excluído os arquivos temporários da Internet após a última varredura.

Para examinar sem usar as configurações de varredura manual:

1. No menu Avançado, clique em **Início**.
2. No painel Início, clique em **Varredura**.
3. Em **Locais para fazer a varredura**, selecione as caixas de seleção ao lado dos arquivos, das pastas e das unidades que você deseja examinar.
4. Em **Opções**, selecione as caixas de seleção ao lado dos tipos de arquivos que você deseja examinar.
5. Clique em **Fazer varredura agora**. Quando a varredura for concluída, um resumo mostrará o número de itens examinados e detectados, o número de itens limpos e quando ocorreu a última varredura.
6. Clique em **Concluir**.

Observação: Essas opções não são salvas.

Varredura no Windows Explorer

Você pode fazer a varredura em busca de vírus e outras ameaças nos arquivos, nas pastas ou nas unidades selecionadas dentro do Windows Explorer.

Para fazer a varredura de arquivos no Windows Explorer:

1. Abra o Windows Explorer.
2. Clique com o botão direito do mouse no arquivo, na pasta ou na unidade em que a varredura será feita e clique em **Fazer varredura**. Todas as opções de varredura padrão são selecionadas para proporcionar uma varredura completa.

Configurando varreduras manuais

Ao executar uma varredura manual ou programada, você pode especificar os tipos de arquivos a serem examinados, os locais a serem examinados e o momento da execução de uma varredura.

Configurar o tipo de arquivo a ser examinado

Você pode configurar o tipo de arquivo a ser examinado.

Para configurar o tipo de arquivo a ser examinado:

1. No menu Avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Computador e arquivos**.
3. Em **Proteção contra vírus**, clique em **Avançado**.
4. No painel Proteção contra vírus, clique em **Varredura manual**.
5. Selecione ou limpe as seguintes caixas de seleção:
   - **Fazer varredura para vírus desconhecidos usando heurística**: É feita uma correspondência entre arquivos e assinaturas de vírus conhecidos para detectar sinais de vírus não identificados. Essa opção proporciona a varredura mais completa, mas geralmente é mais lenta do que a varredura normal.
   - **Fazer varredura em arquivos .zip e outros arquivos compactados**: Detecta e remove os vírus nos arquivos .zip e em outros arquivos compactados. Às vezes, os autores de vírus colocam os vírus em arquivos .zip e depois os inserem em outros arquivos .zip para tentar burlar os mecanismos antivírus.
   - **Fazer a varredura para spyware e programas potencialmente indesejados**: São detectados e removidos spywares, adwares e outros programas com potencial de coletar e transmitir dados sem a sua permissão.
   - **Fazer varredura e remover cookies de rastreamento**: São detectados e removidos os cookies com potencial de coletar e transmitir dados sem a sua permissão. Um cookie identifica os usuários quando eles visitam uma página da Web.
   - **Fazer a varredura para rootkits e outros programas furtivos**: Detecta e remove qualquer rootkit ou outro programa que esteja oculto no Windows.
6. Clique em um dos seguintes botões:
   - **Todos os arquivos (recomendável)**: É feita uma varredura em cada tipo de arquivo usado em seu computador. Use essa opção para obter a varredura mais completa.

- **Apenas arquivos de programa e documentos**: É feita uma varredura apenas nos arquivos de programa e nos documentos.

7 Clique em **OK**.

Configurar os locais a serem examinados

Você pode configurar os locais a serem examinados em varreduras manuais ou programadas.

Para configurar onde examinar:

1 No menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador e arquivos**.

3 Em **Proteção contra vírus**, clique em **Avançado**.

4 No painel Proteção contra vírus, clique em **Varredura manual**.

5 Em **Local padrão para fazer a varredura**, selecione os arquivos, as pastas e as unidades que você deseja examinar.

   Para obter a varredura mais completa possível, certifique-se de que **Arquivos importantes** esteja selecionado.

6 Clique em **OK**.

Programar varreduras

Você pode programar as varreduras para verificar completamente o seu computador em busca de vírus e outras ameaças em intervalos específicos.

Para programar uma varredura:

1 No menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador e arquivos**.

3 Em **Proteção contra vírus**, clique em **Avançado**.

4 No painel Proteção contra vírus, clique em **Varredura programada**.

5 Certifique-se de que **Ativar varredura programada** esteja selecionado.

6 Selecione a caixa de seleção ao lado do dia da semana em que a varredura será executada.

7 Clique nos valores nas listas de hora de início para especificar uma hora de início.

8 Clique em **OK**.

Dica: Para usar a programação padrão, clique em **Redefinir**.

CAPÍTULO 16

Adminstrando o VirusScan

Você pode remover itens de listas confiáveis, gerenciar os programas, os cookies e os arquivos em quarentena, visualizar eventos e registros, bem como relatar atividades suspeitas para a McAfee.

Neste capítulo

Gerenciando listas confiáveis

Quando você confia em um SystemGuard, programa, sobrecarga de buffer ou programa de e-mail, o item é adicionado a uma lista confiável para que não seja mais detectado.

Se você confiar em um programa por engano ou desejar que ele seja detectado, será necessário removê-lo da lista.

Gerenciar listas confiáveis

Quando você confia em um SystemGuard, programa, sobrecarga de buffer ou programa de e-mail, o item é adicionado a uma lista confiável para que não seja mais detectado.

Se você confiar em um programa por engano ou desejar que ele seja detectado, será necessário removê-lo da lista.

Para remover itens das listas confiáveis:

1 No menu Avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Computador e arquivos**.

3 Em **Proteção contra vírus**, clique em **Avançado**.

4 No painel Proteção contra vírus, clique em **Listas de confiáveis**.

5 Na lista, selecione um SystemGuard, programa, sobrecarga de buffer ou programa de e-mail confiável para visualizar seus itens e status de confiança.

6 Em **Detalhes**, exiba as informações sobre o item.

7 Em **Desejo**, clique em uma ação.

8 Clique em **OK**.

Gerenciando programas, cookies e arquivos em quarentena

Os programas, os cookies e os arquivos em quarentena podem ser restaurados, excluídos ou enviados à McAfee para análise.

Restaurar programas, cookies e arquivos em quarentena

Se necessário, você poderá restaurar programas, cookies e arquivos em quarentena.

Para restaurar programas, cookies e arquivos em quarentena:

1. No menu Avançado, clique em **Restaurar**.
2. No painel Restaurar, clique em **Programas e cookies** ou **Arquivos**, conforme apropriado.
3. Selecione os programas, os cookies ou os arquivos em quarentena que você deseja restaurar.
4. Para obter mais informações sobre o vírus que está em quarentena, clique no respectivo nome de detecção em **Detalhes**. A Biblioteca de informações sobre vírus aparece com a descrição do vírus.
5. Em **Desejo**, clique em **Restaurar**.

Remover programas, cookies e arquivos em quarentena

Você pode remover programas, cookies e arquivos que estejam em quarentena.

Para remover programas, cookies e arquivos em quarentena:

1. No menu Avançado, clique em **Restaurar**.
2. No painel Restaurar, clique em **Programas e cookies** ou **Arquivos**, conforme apropriado.
3. Selecione os programas, os cookies ou os arquivos em quarentena que você deseja restaurar.
4. Para obter mais informações sobre o vírus que está em quarentena, clique no respectivo nome de detecção em **Detalhes**. A Biblioteca de informações sobre vírus aparece com a descrição do vírus.
5. Em **Desejo**, clique em **Remover**.

Enviar programas, cookies e arquivos em quarentena para a McAfee

Você pode enviar programas, cookies e arquivos em quarentena à McAfee para análise.

Observação: Se o arquivo em quarentena que você está enviando exceder um tamanho máximo, o arquivo poderá ser rejeitado. Na maioria dos casos, isso não ocorre.

Para enviar os programas ou os arquivos em quarentena para a McAfee:

1. No menu Avançado, clique em **Restaurar**.
2. No painel Restaurar, clique em **Programas e cookies** ou **Arquivos**, conforme apropriado.
3. Selecione os programas, os cookies ou os arquivos em quarentena que você deseja enviar para a McAfee.
4. Para obter mais informações sobre o vírus que está em quarentena, clique no respectivo nome de detecção em **Detalhes**. A Biblioteca de informações sobre vírus aparece com a descrição do vírus.
5. Em **Desejo**, clique em **Enviar para a McAfee**.

Exibindo eventos e registros recentes

Eventos e registros recentes exibem os eventos de todos os produtos McAfee instalados.

Em Eventos recentes, você pode ver os últimos 30 eventos significativos que ocorreram em seu computador. Você pode restaurar os programas bloqueados, reativar a varredura em tempo real e confiar em sobrecargas de buffer.

Você também pode exibir registros, que gravam todos os eventos ocorridos nos últimos 30 dias.

Exibir eventos

Em Eventos recentes, você pode ver os últimos 30 eventos significativos que ocorreram em seu computador. Você pode restaurar os programas bloqueados, reativar a varredura em tempo real e confiar em sobrecargas de buffer.

Para exibir eventos:

1. No Menu avançado, clique em **Relatórios e registros**.
2. No painel Relatórios e registros, clique em **Eventos recentes**.
3. Selecione o evento que você deseja exibir.
4. Em **Detalhes**, exiba as informações sobre o evento.
5. Em **Desejo**, clique em uma ação.

Exibir registros

Os registros gravam todos os eventos ocorridos nos últimos 30 dias.

Para exibir registros:

1. No Menu avançado, clique em **Relatórios e registros**.
2. No painel Relatórios e registros, clique em **Eventos recentes**.
3. No painel Eventos recentes, clique em **Exibir registro**.
4. Selecione o tipo de registro que você deseja exibir e, em seguida, selecione um registro.
5. Em **Detalhes**, exiba as informações sobre o registro.

Relatando automaticamente informações anônimas

Você pode enviar anonimamente à McAfee informações sobre rastreamento de vírus, de programas potencialmente indesejados e de hacker. Essa opção fica disponível apenas durante a instalação.

Nenhuma informação pessoal identificável é coletada.

Relatar à McAfee

Você pode enviar à McAfee informações sobre rastreamento de vírus, de programas potencialmente indesejados e de hacker. Essa opção fica disponível apenas durante a instalação.

Para relatar automaticamente informações anônimas:

1 Durante a instalação do VirusScan, aceite o padrão **Enviar informações anônimas**.

2 Clique em **Avançar**.

Noções básicas sobre alertas de segurança

Se a varredura em tempo real detectar uma ameaça, um alerta de vírus será exibido. Com a maioria dos vírus, cavalos de Tróia, scripts e worms, a varredura em tempo real tenta limpar automaticamente o arquivo e envia um alerta a você. Com programas potencialmente indesejados e SystemGuards, a varredura em tempo real detecta o arquivo ou a alteração e envia um alerta a você. Com sobrecarga de buffer, cookies de rastreamento e atividade de scripts, a varredura em tempo real bloqueia a atividade e envia um alerta a você.

Esses alertas podem ser agrupados em três tipos básicos.

- Alerta vermelho
- Alerta amarelo
- Alerta verde

Você pode então escolher como gerenciar arquivos detectados, e-mails detectados, scripts suspeitos, worms em potencial, programas potencialmente indesejados, SystemGuards ou sobrecargas de buffer.

Gerenciar alertas

A McAfee emprega uma gama de alertas para ajudá-lo a gerenciar a sua segurança. Esses alertas podem ser agrupados em três tipos básicos.

- Alerta vermelho
- Alerta amarelo
- Alerta verde

Alerta vermelho

Um alerta vermelho requer uma resposta sua. Em alguns casos, a McAfee não pode determinar como responder automaticamente a uma determinada atividade. Nesses casos, o alerta vermelho descreve a atividade em questão e oferece uma ou mais opções para seleção.

Alerta amarelo

Um alerta amarelo é uma notificação não crítica que geralmente requer uma resposta sua. O alerta amarelo descreve a atividade em questão e oferece uma ou mais opções para seleção.

Alerta verde

Na maioria dos casos, um alerta verde fornece informações básicas sobre um evento e não requer uma resposta.

Configurando opções de alerta

Se você optar por não mostrar um alerta novamente e mais tarde mudar de idéia, é possível voltar atrás e configurar esse alerta para que apareça de novo. Para obter mais informações sobre como configurar opções de alerta, consulte a documentação do SecurityCenter.

CAPÍTULO 17

Ajuda adicional

Este capítulo descreve as perguntas freqüentes e os cenários de solução de problemas.

Neste capítulo

Perguntas freqüentes

Esta seção fornece as respostas para as perguntas mais freqüentes.

Uma ameaça foi detectada, o quê devo fazer?

A McAfee usa os alertas para ajudá-lo a gerenciar a sua segurança. Esses alertas podem ser agrupados em três tipos básicos.

- Alerta vermelho
- Alerta amarelo
- Alerta verde

Você pode escolher como gerenciar arquivos detectados, e-mails detectados, scripts suspeitos, worms em potencial, programas potencialmente indesejados, SystemGuards ou sobrecargas de buffer.

Para obter mais informações sobre o gerenciamento de ameaças específicas, consulte a Biblioteca de informações sobre vírus em: http://us.mcafee.com/virusInfo/default.asp?affid=.

Tópicos relacionados

- Noções básicas sobre alertas de segurança (página 107)

Posso usar o VirusScan com navegadores Netscape, Firefox e Opera?

Você pode usar o Netscape, o Firefox e o Opera como seu navegador de Internet padrão, mas deve ter o Microsoft® Internet Explorer 6.0 ou posterior instalado em seu computador.

Preciso estar conectado à Internet para fazer uma varredura?

Você não precisa estar conectado à Internet para fazer uma varredura, mas deve se conectar ao menos uma vez por semana para receber as atualizações da McAfee.

O VirusScan faz a varredura de anexos de e-mail?

Se você tiver a varredura em tempo real e a proteção de e-mail ativadas, todos os anexos serão examinados assim que a mensagem de e-mail chegar.

O VirusScan faz a varredura de arquivos compactados?

O VirusScan faz a varredura de arquivos .zip e outros arquivos compactados.

Por que ocorrem erros na varredura de e-mails enviados?

Durante a varredura das mensagens de e-mail enviadas, podem ocorrer estes tipos de erros:

- Erro de protocolo. O servidor de e-mail rejeitou uma mensagem de e-mail.
  Se ocorrer um erro de protocolo ou sistema, as demais mensagens de e-mail dessa sessão serão processadas e enviadas ao servidor.
- Erro de conexão. A conexão ao servidor de e-mail foi interrompida.
  Caso ocorra um erro de conexão, verifique se o seu computador está conectado à Internet e, em seguida, tente enviar a mensagem novamente a partir da lista de itens **Enviados** do programa de e-mail.
- Erro do sistema. Ocorreu uma falha na manipulação de arquivos ou outro erro de sistema.
- Erro de conexão SMTP criptografada. Foi detectada uma conexão SMTP criptografada em seu programa de e-mail.
  Se ocorrer um erro de conexão SMTP criptografada, desative a conexão SMTP criptografada em seu programa de e-mail para garantir que as suas mensagens de e-mail serão examinadas.

Caso o tempo limite seja excedido durante o envio de mensagens de e-mail, desative a varredura de e-mails enviados ou encerre a conexão SMTP criptografada em seu programa de e-mail.

Tópicos relacionados

- Configurar a proteção de e-mail (página 92)

Solução de problemas

Esta seção fornece ajuda para os problemas gerais que você pode encontrar.

Um vírus não pode ser limpo nem excluído

Você deve limpar manualmente o seu computador contra alguns vírus. Tente reiniciar o seu computador e, em seguida, fazer a varredura novamente.

Se o seu computador não puder limpar nem excluir um vírus, consulte a Biblioteca de informações sobre vírus em: http://us.mcafee.com/virusInfo/default.asp?affid=.

Se você precisar de ajuda adicional, consulte o Atendimento ao cliente McAfee no site da McAfee na Web.

Observação: Os vírus não podem ser limpos nos CD-ROMs, nos DVDs e nos disquetes protegidos contra gravação.

Após a reinicialização, um item ainda não pode ser removido

Depois de examinar e remover os itens, talvez você precise reiniciar o computador.

Se o item não for removido depois de reiniciar o computador, envie o arquivo para a McAfee.

Observação: Os vírus não podem ser limpos nos CD-ROMs, nos DVDs e nos disquetes protegidos contra gravação.

Tópicos relacionados

- Gerenciando programas, cookies e arquivos em quarentena (página 103)

Há componentes ausentes ou corrompidos

Algumas situações podem fazer com que o VirusScan seja instalado incorretamente:

- O seu computador não possui espaço em disco ou memória suficientes. Verifique se o seu computador atende aos requisitos de sistema para executar esse software.
- Seu navegador da Internet está configurado incorretamente.
- Você possui uma conexão instável com a Internet. Verifique sua conexão ou tente novamente mais tarde.
- Os arquivos estão ausentes ou ocorreu falha na instalação.

A melhor solução é resolver esses problemas potenciais e, em seguida, reinstalar o VirusScan.

CAPÍTULO 18

McAfee Personal Firewall

O Personal Firewall oferece proteção avançada para seu computador e seus dados pessoais. O Personal Firewall estabelece uma barreira entre o seu computador e a Internet, monitorando de forma silenciosa o tráfego da Internet em busca de atividades suspeitas.

Neste capítulo

Recursos

O Personal Firewall fornece proteção de firewall completa de entrada e saída, confia automaticamente em programas úteis e ajuda a bloquear spyware, Cavalos de Tróia e registradores de digitação. O Firewall permite que você se defenda de sondagens e invasões de hackers, monitore a atividade de Internet e rede, além de alertar você sobre eventos suspeitos ou hostis, fornecer informações detalhadas sobre tráfego de Internet e complementar as defesas antivírus.

Níveis de proteção padrão e personalizado

Proteja-se contra atividades suspeitas e invasões, utilizando a configuração padrão de proteção do Firewall ou personalize o Firewall para atender às suas necessidades de segurança.

Recomendações em tempo real

Receba recomendações de forma dinâmica para ajudá-lo a determinar se os programas devem ter acesso à Internet ou se o tráfego de rede é confiável.

Gerenciamento inteligente de acesso para programas

Gerencie o acesso à Internet para programas, por meio de alertas e Registros de eventos ou configure permissões de acesso para programas específicos, a partir do painel de Permissões do programa do Firewall.

Proteção para jogos

Evite que os alertas relativos a tentativas de invasão e atividades suspeitas o distraiam enquanto você joga em tela inteira, e configure o Firewall para exibir alertas depois da conclusão dos jogos de computador.

Proteção de inicialização do computador

Antes de o Windows ser aberto, o Firewall protege o computador de tentativas de invasão, programas indesejados e tráfego de rede.

Controle da porta de serviço do sistema

As portas de serviço do sistema podem fornecer uma forma de comunicação clandestina com o computador. O Firewall permite que você crie e gerencie portas de serviço abertas e fechadas do sistema exigidas por alguns programas.

Gerenciamento de conexões do computador

Libere e proíba conexões remotas e endereços IP que podem se conectar ao seu computador.

Integração com informações do HackerWatch

O HackerWatch é um hub de informações de segurança que rastreia padrões de invasão e ações de hackers globalmente, fornecendo as informações mais atualizadas sobre os programas no seu computador. É possível visualizar estatísticas de portas de Internet e eventos de segurança globais.

Bloqueio do Firewall

Bloqueie instantaneamente todo o tráfego de entrada e de saída da rede entre o computador e a Internet.

Restauração do Firewall

Restaure instantaneamente as configurações originais de proteção do Firewall. Se o Personal Firewall se comportar de uma forma que você não consiga corrigir, será possível restaurá-lo para as configurações padrão.

Detecção avançada de Cavalos de Tróia

Combine gerenciamento de conexão de aplicativos com um banco de dados aprimorado para detectar e impedir que aplicativos possivelmente mal-intencionados, como Cavalos de Tróia, acessem a Internet e transmitam seus dados pessoais.

Registro de eventos

Especifique se deseja ativar ou desativar o registro e, se ativado, que tipo de eventos registrar. O registro de eventos permite que você verifique eventos recentes de entrada e de saída. Também é possível exibir eventos de detecção de invasões.

Monitoramento do tráfego de Internet

Revise mapas gráficos de fácil leitura, que mostram a origem de ataques e tráfego hostis no mundo todo. Além disso, localize informações detalhadas sobre o proprietário e dados geográficos de endereços IP de origem. Analise também o trafego de entrada e saída, monitore a largura de banda e as atividades dos programas.

Prevenção de invasões

Proteja sua privacidade com prevenção de invasões contra possíveis ameaças de Internet. Utilizando a funcionalidade heurística, a McAfee fornece uma terceira camada de proteção, através do bloqueio de itens que exibem sintomas de ataques ou características de atividades de hackers.

Análise sofisticada de tráfego

Analise o tráfego de entrada e saída de Internet e as conexões de programas, inclusive aquelas que estão ouvindo ativamente as conexões abertas. Isso permite que você veja e tome providências em relação a programas que possam estar vulneráveis a invasões.

Iniciando o Firewall

Assim que você instalar o Firewall, seu computador estará protegido contra invasões e tráfego de rede indesejado. Além disso, você estará pronto para lidar com alertas e gerenciar o acesso de entrada e saída da Internet para programas conhecidos e desconhecidos. As Recomendações inteligentes e o nível de segurança Padrão são ativados automaticamente.

Você pode desativar o Firewall no painel Internet & Configuração de rede, mas seu computador não estará mais protegido contra invasões e tráfego de rede indesejado, e você não poderá gerenciar eficientemente as conexões de entrada e saída com a Internet. Se você precisar desativar a proteção de firewall, faça-o temporariamente e apenas quando necessário. Você também pode ativar o Firewall a partir do painel Internet & Configuração de rede.

O Firewall desativa automaticamente o Windows® Firewall e se define como o firewall padrão.

Observação: Para configurar o Firewall, abra o painel Configuração de rede e Internet.

Iniciar proteção de firewall

A ativação da proteção de firewall defende o computador contra invasões e tráfego de rede indesejado, além de ajudar a gerenciar as conexões de entrada e de saída da Internet.

Para ativar a proteção por firewall:

1 No painel do McAfee Security Center, execute um dos procedimentos a seguir:
   - Clique em **Internet & rede** e, em seguida, em **Configurar**.
   - Clique em **Menu avançado**, depois em **Configurar** no painel **Início** e, em seguida, aponte para **Internet & rede**.

2 No painel **Configuração de Internet & rede**, em **Proteção de firewall**, clique em **Ligado**.

Interromper proteção de firewall

O desativamento da proteção de firewall deixa o computador vulnerável a invasões e tráfego de rede indesejado. Sem a proteção de firewall ativada, não é possível gerenciar conexões de Internet de entrada e saída.

Para desativar a proteção de firewall:

1. No painel do McAfee Security Center, execute um dos procedimentos a seguir:
   - Clique em **Internet & rede** e, em seguida, em **Configurar**.
   - Clique em **Menu avançado**, depois em **Configurar** no painel **Início** e, em seguida, aponte para **Internet & rede**.
2. No painel **Configuração de Internet & rede**, em **Proteção de firewall**, clique em **Desligado**.

Trabalhando com alertas

O Firewall utiliza uma gama de alertas para ajudá-lo a gerenciar sua segurança. Esses alertas podem ser agrupados em quatro tipos básicos.

- Alerta sobre Cavalo de Tróia
- Alerta vermelho
- Alerta amarelo
- Alerta verde

Os alertas também podem conter informações para ajudar o usuário a decidir o que fazer com os alertas ou obter informações sobre os programas em execução no computador.

Sobre alertas

O Firewall tem quatro tipos básicos de alertas. Alguns desses alertas incluem informações para ajudá-lo a obter informações sobre programas executados em seu computador.

Alerta sobre Cavalo de Tróia

Um Cavalo de Tróia parece ser um programa legítimo, mas pode atrapalhar, danificar ou fornecer acesso não autorizado ao seu computador. O alerta de Cavalo de Tróia aparece quando o Firewall detecta e bloqueia um Cavalo de Tróia no computador, e recomenda que você faça uma varredura para buscar outras ameaças. Esse alerta é exibido em todos os níveis de segurança, exceto no nível Aberto ou quando as Recomendações inteligentes estão desativadas.

Alerta vermelho

O tipo de alerta mais comum é o alerta vermelho, que geralmente exige uma resposta do usuário. Como o Firewall, em alguns casos, não é capaz de determinar automaticamente uma ação específica para uma atividade do programa ou evento da rede, o alerta primeiramente descreve a atividade do programa ou evento de rede em questão, seguida por uma ou mais opções às quais você deve responder. Se as Recomendações inteligentes estiverem ativadas, os programas serão adicionados ao painel Permissões do programa.

As descrições de alertas a seguir são as mais comuns:

- **O programa solicita acesso à Internet**: O firewall detecta um programa tentando acessar a Internet.
- **O programa foi modificado**: O Firewall detecta um programa que foi modificado de alguma maneira, talvez como resultado de uma atualização on-line.
- **Programa bloqueado**: O firewall bloqueia um programa porque ele está na lista do painel Permissões do programa.

Dependendo de suas configurações e das atividades do programa ou eventos de rede, as opções a seguir são as mais comuns:

- **Conceder acesso**: Permite que um programa do computador acesse a Internet. A regra é adicionada à página Permissões do programa.
- **Conceder acesso uma única vez**: Permite que um programa em seu computador acesse a Internet temporariamente. Por exemplo, a instalação de um novo programa pode exigir acesso somente uma vez.
- **Bloquear acesso**: Impede que um programa acesse a Internet.

- **Conceder somente acesso de saída**: Permite somente uma conexão de saída à Internet. Esse alerta aparece normalmente quando os níveis de segurança Rígido e Oculto estão definidos.
- **Confiar nesta rede**: Permitir tráfego de entrada e de saída de uma rede. A rede é adicionada à seção de endereços IP confiáveis.
- **Não confiar nesta rede agora**: Bloquear tráfego de entrada e de saída de uma rede.

Alerta amarelo

O alerta amarelo é uma notificação menos importante, que informa a respeito de um evento de rede detectado pelo firewall. Por exemplo, o alerta **Nova rede detectada** é exibido quando o firewall é executado pela primeira vez ou quando um computador com o firewall instalado é conectado a uma nova rede. Você pode escolher confiar ou não confiar na rede. Se a rede for confiável, o Firewall permite o tráfego a partir de qualquer outro computador da rede e a adiciona aos Endereços IP confiáveis.

Alerta verde

Na maioria dos casos, um alerta verde fornece informações básicas sobre um evento e não requer uma resposta. Os alertas verdes ocorrem normalmente quando os níveis de segurança Padrão, Rígido, Oculto e Bloqueado estão definidos. As descrições de alertas verdes são as seguintes:

- **O programa foi modificado**: Informa que um programa ao qual você concedeu acesso à Internet anteriormente foi modificado. Você pode optar por bloquear o programa, mas se decidir não responder, a alerta desaparecerá da área de trabalho e o programa continuará a ter acesso.
- **O programa obteve acesso à Internet**: Notifica que o acesso à Internet foi concedido a um programa. Você pode optar por bloquear o programa, mas se você não responder, a alerta desaparece e o programa continua a acessar a Internet.

Assistência ao usuário

Muitos alertas do firewall contêm informações adicionais para ajudá-lo a gerenciar a segurança do computador. Entre elas estão as seguintes:

- **Saiba mais sobre este programa**: Acessar o site de segurança global da McAfee na Web para obter informações sobre um programa detectado pelo Firewall em seu computador.

- **Informe a McAfee sobre este programa**: Enviar informações à McAfee sobre um arquivo desconhecido que o firewall detectou em seu computador.
- **A McAfee recomenda**: Informações sobre o gerenciamento de alertas. Por exemplo, um alerta pode recomendar que você conceda acesso a um programa.

Gerenciando alertas informativos

O Firewall permite que você exiba ou oculte alertas informativos durante certos eventos.

Exibir alertas durante jogos

Por padrão, o Firewall impede que os alertas informativos sejam exibidos durante jogos em tela inteira. No entanto, você pode configurar o Firewall para que exiba alertas informativos durante os jogos, quando forem detectadas tentativas de invasão ou atividades suspeitas.

Para exibir alertas durante jogos:

1 No painel Tarefas comuns, clique em **Menu avançado**.

2 Clique em **Configurar**.

3 No painel Configuração do SecurityCenter, clique em **Alertas**.

4 Clique em **Avançado**.

5 No painel **Opções de alerta**, selecione **Mostrar alertas informativos quando o modo de jogo for detectado**.

Ocultar alertas informativos

Os alertas informativos avisam a você sobre eventos que não exigem resposta imediata.

Para ocultar alertas informativos:

1 No painel Tarefas comuns, clique em **Menu avançado**.

2 Clique em **Configurar**.

3 No painel Configuração do SecurityCenter, clique em **Alertas**.

4 Clique em **Avançado**.

5 No painel **Configuração do SecurityCenter**, clique em **Alertas informativos**.

6 No painel **Alertas informativos**, execute um dos procedimentos a seguir:

- Selecione um tipo de alerta a ser ocultado.
- Selecione **Ocultar alertas informativos** para ocultar todos os alertas informativos.

7 Clique em **OK**.

CAPÍTULO 19

Configurando a proteção do Firewall

O Firewall oferece vários métodos para gerenciar sua segurança e personalizar a maneira como você deseja responder a eventos e alertas de segurança.

Quando você instala o Firewall pela primeira vez, o nível de proteção é definido como segurança Padrão. Para a maioria das pessoa, essa configuração atende a todas as necessidades de segurança. No entanto, o Firewall oferece outros níveis, que vão do altamente restritivo ao altamente permissivo.

O Firewall também oferece a oportunidade de receber recomendações sobre alertas e acesso de programas à Internet.

Neste capítulo

Gerenciando os níveis de segurança do Firewall

Você pode configurar os níveis de segurança para controlar o grau em que deseja gerenciar e responder a alertas quando o Firewall detectar tráfego de rede indesejado e conexões de Internet de entrada e saída. Por padrão, o nível de segurança Padrão é ativado.

Quando o nível de segurança Padrão e as Recomendações inteligentes estão ativadas, alertas vermelhos fornecem as opções para conceder ou bloquear o acesso de programas desconhecidos ou modificados. Quando programas conhecidos são detectados, são exibidos alertas informativos verdes e o acesso é concedido automaticamente. A concessão de acesso permite que um programa crie conexões de saída e escute as conexões de entrada não solicitadas.

Geralmente, quanto mais restritivo for o nível de segurança (Oculto e Rígido), maior será o número de opções e alertas exibidos com os quais você precisará lidar.

O Firewall utiliza cinco níveis de segurança. Do mais restritivo ao menos restritivo, esses níveis são os seguintes:

- **Bloqueado**: Bloqueia todas as conexões com a Internet.
- **Oculto**: Bloqueia todas as conexões de entrada com a Internet.
- **Rígido**: Os alertas exigem que você responda a todas as solicitações de conexões de entrada e saída com a Internet.
- **Padrão**: Os alertas notificam quando programas desconhecidos ou novos solicitam acesso à Internet.
- **Confiável**: Permite todas as conexões de entrada e saída com a Internet e adiciona-as automaticamente ao painel Permissões do programa.
- **Aberto**: Permite todas as conexões de entrada e saída com a Internet.

O Firewall também permite que você redefina imediatamente seu nível de segurança como Padrão no painel Restaurar padrões de proteção do Firewall.

Definir nível de segurança como Bloqueado

Quando o nível de segurança é definido como Bloqueado, todas as conexões de rede de entrada e de saída são bloqueadas, incluindo o acesso a sites da Web, e-mails e atualizações de segurança. Este nível de segurança tem o mesmo resultado que a remoção de sua conexão com a Internet. Use esta configuração para bloquear as portas definidas como abertas no painel Serviços do sistema. Durante o Bloqueio, os alertas podem continuar a solicitar que você bloqueie os programas.

Para definir o nível de segurança do firewall como Bloqueado:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Bloqueado**.
3. Clique em **OK**.

Definir nível de segurança como Oculto

Quando o nível de segurança do firewall é definido como Oculto, todas as conexões de rede de entrada são bloqueadas, exceto as portas abertas. Esta configuração oculta totalmente a presença do computador na Internet. Quando o nível de segurança é definido como Oculto, o firewall avisa você quando novos programas tentam estabelecer conexões de saída com a Internet ou recebem solicitações de conexão de entrada. Os programas bloqueados e adicionados aparecem no painel Permissões do programa.

Para definir o nível de segurança do firewall como Oculto:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Oculto**.
3. Clique em **OK**.

Definir nível de segurança como Rígido

Quando o nível de segurança é definido como Rígido, o firewall informa quando novos programas tentam estabelecer conexões de saída com a Internet ou recebem solicitações de conexão de entrada. Os programas bloqueados e adicionados aparecem no painel Permissões do programa. Quando o nível de segurança é definido como Rígido, o programa solicita apenas o tipo de acesso exigido naquele momento, por exemplo, acesso apenas de saída, que você pode conceder ou bloquear. Mais tarde, se o programa exigir uma conexão de saída e também de entrada, você pode conceder acesso total no painel Permissões do programa.

Para definir o nível de segurança do firewall como Rígido:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Rígido**.
3. Clique em **OK**.

Definir nível de segurança como Padrão

Padrão é o nível de segurança padrão e recomendado.

Quando o nível de segurança é definido como Padrão, o Firewall monitora conexões de entrada e de saída e avisa quando novos programas tentam acessar a Internet. Os programas bloqueados e adicionados aparecem no painel Permissões do programa.

Para definir o nível de segurança do firewall como Padrão:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Padrão**.
3. Clique em **OK**.

Definir nível de segurança como Confiável

Quando o nível de segurança do firewall é definido como Confiável, todas as conexões de rede de entrada são permitidas. No nível Confiável, o firewall concede acesso a todos os programas automaticamente e os adiciona à lista de programas permitidos nas Permissões do programa.

Para definir o nível de segurança do firewall como Confiável

1 No painel Internet & Configuração de rede, clique em **Avançado**.

2 No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Confiável**.

3 Clique em **OK**.

Configurando as Recomendações inteligentes para alertas

Você pode configurar o Firewall para incluir, excluir ou exibir recomendações em alertas referentes a programas que tentam acessar a Internet.

A ativação das recomendações inteligentes ajuda você a decidir como lidar com alertas. Quando as Recomendações inteligentes estão ativadas (e o nível de segurança é Padrão), o Firewall automaticamente permite ou bloqueia programas conhecidos, e alerta você, recomendando uma ação, quando detecta programas desconhecidos e potencialmente perigosos.

Quando as Recomendações inteligentes estão desativadas, o Firewall não concede nem bloqueia acesso à Internet automaticamente, nem recomenda uma ação.

Quando o Firewall está configurado para Somente exibir as recomendações inteligentes, um alerta solicita que você conceda ou bloqueie o acesso, mas sugere uma ação.

Ativar Recomendações inteligentes

A ativação das recomendações inteligentes ajuda você a decidir como lidar com alertas. Quando as Recomendações inteligentes estão ativadas, o Firewall autoriza ou bloqueia programas automaticamente e envia alertas sobre programas não reconhecidos ou potencialmente perigosos.

Para ativar as Recomendações inteligentes:

1 No painel Internet & Configuração de rede, clique em **Avançado**.

2 No painel Nível de segurança, em **Recomendações inteligentes**, selecione **Ativar Recomendações inteligentes**.

3 Clique em **OK**.

Desativar Recomendações inteligentes

Quando você desativa as Recomendações inteligentes, os alertas excluem a assistência para gerenciamento de alertas e acesso para programas. Se as Recomendações inteligentes forem desativadas, o firewall continuará a autorizar ou bloquear programas automaticamente e enviará alertas sobre programas não reconhecidos ou potencialmente perigosos. E se detectar um novo programa suspeito ou conhecido com uma possível ameaça, o Firewall bloqueará o acesso do programa à Internet automaticamente.

Para desativar as Recomendações inteligentes:

1 No painel Internet & Configuração de rede, clique em **Avançado**.

2 No painel Nível de segurança, em **Recomendações inteligentes**, selecione **Desativar Recomendações inteligentes**.

3 Clique em **OK**.

Somente exibir as recomendações inteligentes

A exibição das Recomendações inteligentes ajuda você a decidir como lidar com alertas sobre programas não reconhecidos ou potencialmente perigosos. Quando as Recomendações inteligentes são definidas como **Somente exibir**, as informações sobre como lidar com alertas são exibidas, mas, diferentemente da opção **Ativar Recomendações inteligentes**, as recomendações exibidas não são aplicadas automaticamente e o acesso dos programas não é concedido ou bloqueado automaticamente. Ao invés disso, os alertas fornecem recomendações que ajudam você a decidir se permite ou bloqueia os programas.

Para Somente exibir as recomendações inteligentes

1 No painel Internet & Configuração de rede, clique em **Avançado**.

2 No painel Nível de segurança, em **Recomendações inteligentes**, selecione **Somente exibir**.

3 Clique em **OK**.

Otimizando a segurança do Firewall

Há muitas maneiras pelas quais a segurança de seu computador pode ser comprometida. Por exemplo, alguns programas podem tentar se conectar à Internet antes que o Windows® seja iniciado. Além disso, usuários sofisticados podem executar ping em seu computador para verificar se ele está conectado a uma rede. O Firewall permite que você se defenda contra esses dois tipos de invasão, permitindo que você ative a proteção de inicialização e bloqueie solicitações de ping ICMP. A primeira configuração bloqueia o acesso de programas à Internet enquanto o Windows é iniciado, e a segunda bloqueia solicitações de ping que ajudam outros usuários a detectar seu computador em uma rede.

As configurações de instalação padrão incluem detecção automática para as tentativas mais comuns de invasão, como ataques de Negação de serviço ou explorações. O uso das configurações de instalação padrão garante a sua proteção contra ataques e varreduras. Entretanto, é possível desativar a detecção automática para um ou mais ataques ou procuras no painel de Detecção de intrusão.

Proteja seu computador durante a inicialização

O firewall pode proteger seu computador enquanto o Windows é iniciado. A proteção de inicialização bloqueia todos os programas novos que não tenham sido permitidos anteriormente e exigem acesso à Internet. Depois que o Firewall é iniciado, ele exibe os alertas relevantes para os programas que solicitaram acesso à Internet durante a inicialização e, então, você pode permiti-los ou bloqueá-los. Para utilizar essa opção, seu nível de segurança não pode estar definido como Aberto ou Bloqueado.

Para proteger seu computador durante a inicialização:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Nível de segurança, em Configurações de segurança, selecione **Ativar proteção de inicialização**.
3. Clique em **OK**.

Observação: As conexões e invasões bloqueadas não são registradas enquanto a proteção de inicialização está ativada.

Configurações de solicitações de ping

Usuários de computador podem usar uma ferramenta de ping, que envia e recebe mensagens de Solicitação de Eco ICMP, para determinar se um computador específico está conectado à rede. Você pode configurar o Firewall para impedir ou permitir que usuários de computador executem ping em seu computador.

Para configurar pedidos de ping ICMP:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Nível de segurança, em **Configurações de segurança**, execute um dos procedimentos a seguir:
   - Selecione **Permitir solicitações de ping ICMP** para permitir que seu computador seja detectado na rede por solicitações de ping.
   - Desmarque **Permitir solicitações de ping ICMP** para impedir que seu computador seja detectado na rede por solicitações de ping.
3. Clique em **OK**.

Configurar detecção de invasão

A detecção de invasão (IDS) monitora pacotes de dados em busca de métodos de transferência ou transferências de dados suspeitos. A detecção analisa pacotes de dados e tráfego em busca de padrões específicos usados por invasores. Por exemplo, quando firewall encontra pacotes ICMP, ele os analisa em busca de padrões de tráfego suspeitos, comparando o tráfego ICMP a padrões de ataques conhecidos. O Firewall compara os pacotes com um banco de dados de assinaturas e, se os pacotes forem suspeitos ou nocivos, rejeita os pacotes do computador atacante e, opcionalmente, registra o evento.

As configurações de instalação padrão incluem detecção automática para as tentativas mais comuns de invasão, como ataques de Negação de serviço ou explorações. O uso das configurações de instalação padrão garante a sua proteção contra ataques e varreduras. Entretanto, é possível desativar a detecção automática para um ou mais ataques ou procuras no painel de Detecção de intrusão.

Para configurar a detecção de invasão:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Detecção de invasão**.
3. Em **Detectar tentativas de invasão**, escolha uma das seguintes opções:
   - Selecione um nome para fazer varredura ou detectar automaticamente o ataque.
   - Desmarque um nome para desativar a varredura ou detecção automática de ataque.
4. Clique em **OK.**

Configurar definições do Status de proteção do Firewall

O SecurityCenter rastreia problemas que fazem parte do Status de proteção geral de seu computador. No entanto, o Firewall pode ser configurado para ignorar problemas específicos do computador que podem afetar o Status de proteção. Você pode configurar o SecurityCenter para ignorar quando o Firewall estiver definido no nível de segurança Aberto, quando o Firewall não estiver sendo executado ou quando o Firewall somente de saída não estiver instalado no computador.

Para configurar definições do Status de proteção do Firewall:

1. No painel Tarefas comuns, clique em **Menu avançado**.
2. Clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Alertas**.
4. Clique em **Avançado**.
5. No painel Tarefas comuns, clique em **Menu avançado**.
6. Clique em **Configurar**.
7. No painel Configuração do SecurityCenter, clique em **Status de proteção**.
8. Clique em Avançado.
9. Na janela Problemas ignorados, selecione uma ou mais das seguintes opções:
   - **O nível de segurança do firewall está definido como Aberto.**
   - **O serviço de firewall não está sendo executado.**
   - **O Firewall de saída não está instalado em seu computador.**
10. Clique em **OK**.

Bloqueando e restaurando o Firewall

O bloqueio ajuda a lidar com emergências associadas ao computador, para os usuários que desejam bloquear todo o tráfego a fim de isolar e solucionar o problema no seu computador, ou para aqueles que precisam determinar e não sabem como gerenciar o acesso de um programa à Internet.

Bloquear o Firewall instantaneamente

O bloqueio instantâneo do Firewall bloqueia todo o tráfego de entrada e de saída da rede entre o computador e a Internet. Ele impede que todas as conexões remotas acessem seu computador e impede que todos os programas de seu computador acessem a Internet.

Para bloquear instantaneamente o Firewall e todo o tráfego de rede:

1. No painel Início ou Tarefas comuns, ativando o menu **Básico** ou o **Menu avançado**, clique em **Bloquear Firewall**.
2. No painel Bloquear Firewall, clique em **Bloquear**.
3. Na caixa de diálogo, clique em **Sim** para confirmar que deseja bloquear instantaneamente todo o tráfego de entrada e de saída.

Desbloquear o Firewall instantaneamente

O bloqueio instantâneo do Firewall bloqueia todo o tráfego de entrada e de saída da rede entre o computador e a Internet. Ele impede que todas as conexões remotas acessem seu computador e impede que todos os programas de seu computador acessem a Internet. Depois de Bloquear o Firewall, você pode desbloqueá-lo para permitir o tráfego de rede.

Para desbloquear instantaneamente o Firewall e permitir o tráfego de rede:

1. No painel Início ou Tarefas comuns, ativando o menu **Básico** ou o **Menu avançado**, clique em **Bloquear Firewall**.
2. No painel Bloquear Firewall, clique em **Desbloquear**.
3. Na caixa de diálogo, clique em **Sim** para confirmar que deseja desbloquear o Firewall e permitir o tráfego de entrada e de saída.

Restaurar configurações do Firewall

Você pode restaurar rapidamente o Firewall para suas configurações de proteção originais. Isso define o nível de segurança como padrão, ativa as Recomendações inteligentes, redefine os endereços IP confiáveis e proibidos e remove todos os programas do painel Permissões do programa.

Para restaurar as configurações originais do Firewall:

1. No painel Início ou Tarefas comuns, ativando o menu **Básico** ou o **Menu avançado**, clique em **Restaurar padrões do Firewall**.
2. No painel Restaurar padrões do Firewall, clique em **Restaurar padrões**.
3. No caixa de diálogo Restaurar padrões de proteção do Firewall, clique em **Sim** para confirmar que deseja restaurar as configurações padrão do Firewall.

Definir nível de segurança como Aberto

A definição do nível de segurança como Aberto permite que o firewall conceda acesso a todas as conexões de rede de entrada e de saída. Para conceder acesso a programas bloqueados anteriormente, use o painel Permissões do programa.

Para definir o nível de segurança do firewall como Aberto:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Aberto**.
3. Clique em **OK**.

Observação: Programas bloqueados anteriormente continuarão bloqueados quando o nível de segurança do firewall for definido como **Aberto**. Para evitar isso, você pode mudar a regra do programa para **Acesso total**.

CAPÍTULO 20

Gerenciando programas e permissões

O Firewall permite que você gerencie e crie permissões de acesso para programas existentes e novos que solicitam acesso de entrada e saída à Internet. O Firewall permite que você conceda acesso total ou apenas de saída para os programas. Também é possível bloquear o acesso a programas.

Neste capítulo

Concedendo acesso de programas à Internet

Alguns programas, como navegadores de Internet, precisam acessar a Internet para funcionarem corretamente.

O Firewall permite que você use a página de Permissões do programa para:

- Conceder acesso a programas
- Conceder somente acesso de saída para programas
- Bloquear o acesso de programas

Você também pode conceder acesso total e apenas de saída a partir do registro de Eventos recentes e de Eventos de saída.

Conceder acesso total a um programa

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. O Personal Firewall inclui uma lista de programas aos quais o acesso total é concedido automaticamente, mas você pode modificar essas permissões.

Para conceder acesso total de um programa à Internet:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Permissões do programa**.
3. Em **Permissões do programa**, selecione um programa com acesso **Bloqueado** ou **Somente acesso de saída**.
4. Em **Ação**, clique em **Conceder acesso total**.
5. Clique em **OK**.

Conceder acesso total a um novo programa

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. O Firewall inclui uma lista de programas aos quais o acesso total é concedido automaticamente, mas você pode adicionar um novo programa e modificar suas permissões.

Para conceder acesso total à Internet para um novo programa:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel **Firewall**, clique em **Permissões do programa**.
3. Em **Permissões do programa**, clique em **Adicionar programa permitido**.
4. Na caixa de diálogo **Adicionar programa** procure e selecione o programa que deseja adicionar.
5. Clique em **Abrir**.
6. Clique em **OK**.

   O programa recém-adicionado aparece em **Permissões do programa**.

Observação: Você pode mudar as permissões para um novo programa adicionado do mesmo modo que para um programa existente, selecionando o programa e, em seguida, clicando em **Conceder acesso somente de saída** ou **Bloquear acesso**, em **Ação**.

Conceder acesso total a partir do registro de Eventos recentes

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. Você pode selecionar um programa do registro de Eventos recentes e conceder-lhe acesso total à Internet.

Para conceder acesso total à Internet para um programa a partir do registro de Eventos recentes:

1. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em Eventos recentes, selecione a descrição do evento e clique em **Conceder acesso total**.
3. Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar que deseja conceder acesso total ao programa.

Tópicos relacionados

- Exibir eventos de saída (página 172)

Conceder acesso total a partir do registro de Eventos de saída

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. Você pode selecionar um programa do registro de Eventos de saída e conceder-lhe acesso total à Internet.

Para conceder acesso total à Internet para um programa a partir do registro de Eventos de saída:

1. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Selecione **Internet e rede** e em **Eventos de saída**.
4. No painel Eventos de saída, selecione um endereço IP de origem e clique em **Conceder acesso**.
5. Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar que deseja conceder ao programa acesso total à Internet.

Tópicos relacionados

- Exibir eventos de saída (página 172)

Concedendo somente acesso de saída para programas

Muitos programas em seu computador exigem somente acesso de saída à Internet. O Firewall permite que você conceda aos programas somente acesso de saída à Internet.

Conceder somente acesso de saída para um programa

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. O Personal Firewall inclui uma lista de programas aos quais o acesso total é concedido automaticamente, mas você pode modificar essas permissões.

Para conceder somente acesso de saída para um programa:

1 No painel Internet & Configuração de rede, clique em **Avançado**.
2 No painel Firewall, clique em **Permissões do programa**.
3 Em **Permissões do programa**, selecione um programa com acesso **Bloqueado** ou **Acesso total**.
4 Em **Ação**, clique em **Conceder somente acesso de saída**.
5 Clique em **OK**.

Conceder somente acesso de saída a partir do registro de Eventos recentes

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. Você pode selecionar um programa do registro de Eventos recentes e conceder-lhe somente acesso de saída à Internet.

Para conceder a um programa somente acesso de saída à Internet a partir do registro de Eventos recentes:

1 No painel Tarefas comuns, clique em **Relatórios e registros**.
2 Em Eventos recentes, selecione a descrição do evento e clique em **Conceder somente acesso de saída**.
3 Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar que deseja conceder somente acesso de saída ao programa.

Tópicos relacionados

- Exibir eventos de saída (página 172)

Conceder somente acesso de saída a partir do registro de Eventos de saída

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. Você pode selecionar um programa do registro de Eventos de saída e conceder-lhe somente acesso de saída à Internet.

Para conceder a um programa somente acesso de saída à Internet, a partir do registro de Eventos de saída:

1 No painel Tarefas comuns, clique em **Relatórios e registros**.
2 Em **Eventos recentes**, clique em **Exibir registro**.
3 Selecione **Internet e rede** e em **Eventos de saída**.
4 No painel Eventos de saída, selecione um endereço IP de origem e clique em **Conceder somente acesso de saída**.
5 Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar que deseja conceder somente acesso de saída ao programa.

Tópicos relacionados

- Exibir eventos de saída (página 172)

Bloqueando o acesso de programas à Internet

O Firewall permite que você bloqueie o acesso de programas à Internet. Certifique-se de que o bloqueio de um programa não interromperá sua conexão de rede ou algum outro programa que exija acesso à Internet para funcionar adequadamente.

Bloquear o acesso de um programa

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. O Personal Firewall inclui uma lista de programas aos quais o acesso total é concedido automaticamente, mas você pode bloquear essas permissões.

Para bloquear o acesso de um programa à Internet:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Permissões do programa**.
3. Em **Permissões do programa**, selecione um programa com **Acesso total** ou **Somente acesso de saída**.
4. Em **Ação**, clique em **Bloquear acesso**.
5. Clique em **OK**.

Bloquear o acesso de um novo programa

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. O Personal Firewall inclui uma lista de programas aos quais o acesso total é concedido automaticamente, mas você pode adicionar um novo programa e, a seguir, bloquear seu acesso à Internet.

Para bloquear o acesso de um novo programa à Internet:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Permissões do programa**.
3. Em **Permissões do programa**, clique em **Adicionar programa bloqueado**.
4. Na caixa de diálogo **Adicionar programa** procure e selecione o programa que deseja adicionar.
5. Clique em **Abrir**.
6. Clique em **OK**.

   O programa recém-adicionado aparece em **Permissões do programa**.

Observação: Você pode mudar as permissões para um novo programa adicionado do mesmo modo que para um programa existente, selecionando o programa e, em seguida, clicando em **Conceder somente acesso de saída** ou **Conceder acesso total**, em **Ação**.

Bloquear o acesso a partir do registro de Eventos recentes

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. No entanto, você também pode optar por bloquear o acesso do programas à Internet a partir do registro de Eventos recentes.

Para bloquear o acesso de um programa à Internet a partir do registro de Eventos recentes:

1. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em Eventos recentes, selecione a descrição do evento e clique em **Bloquear acesso**.
3. Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar que deseja bloquear o programa.

Tópicos relacionados

- Exibir eventos de saída (página 172)

Removendo permissões de acesso para programas

Antes de remover uma permissão de programa para um programa, verifique se a ausência dessa permissão não afeta a funcionalidade de seu computador ou a sua conexão de rede.

Remover uma permissão de programa

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. O Personal Firewall inclui uma lista de programas aos quais o acesso total é concedido automaticamente, mas você pode remover programas que foram adicionados automaticamente ou manualmente.

Para remover a permissão de um programa novo:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Permissões do programa**.
3. Em **Permissões do programa**, selecione um programa.
4. Em **Ação**, clique em **Excluir permissões do programa**.
5. Clique em **OK**.

   O programa é removido do painel Permissões do programa.

Observação: O Firewall impede que você modifique alguns programas, minimizando ou desativando ações.

Aprendendo sobre programas

Caso não tenha certeza sobre quais permissões de programa aplicar, você pode obter informações sobre o programa para ajudá-lo a decidir no site HackerWatch da McAfee.

Obter informações sobre programas

Muitos programas em seu computador exigem acesso de entrada e de saída à Internet. O Personal Firewall inclui uma lista de programas aos quais o acesso total é concedido automaticamente, mas você pode modificar essas permissões.

O Firewall pode ajudá-lo a decidir-se entre conceder ou bloquear o acesso de um programa à Internet. Verifique se você está conectado à Internet para que seu navegador inicie o site HackerWatch da McAfee, que fornece informações atualizadas sobre programas, solicitações de acesso à Internet e ameaças à segurança.

Para obter informações sobre programas:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Permissões do programa**.
3. Em **Permissões do programa**, selecione um programa.
4. Em **Ação**, clique em **Saiba mais**.

Obter informações do programa a partir do registro de Eventos de saída

O Personal Firewall permite que você obtenha informações sobre programas que aparecem no registro de Eventos de saída.

Antes de obter informações sobre um programa, certifique-se de possuir uma conexão com a Internet e um navegador da Internet.

Para obter informações do programa a partir do registro de Eventos de saída:

1. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Selecione **Internet e rede** e em **Eventos de saída**.
4. No painel Eventos de saída, selecione um endereço IP de origem e clique em **Saiba mais**.

   Você pode exibir informações sobre o programa no site Hackerwatch. O Hackerwatch fornece informações atualizadas sobre programas, solicitações de acesso à Internet e ameaças à segurança.

Tópicos relacionados

- Exibir eventos de saída (página 172)

CAPÍTULO 21

Gerenciando os serviços do sistema:

Para funcionar corretamente, certos programas (como servidores da Web ou programas de servidor de compartilhamento de arquivos) precisam aceitar conexões não solicitadas de outros computadores através de portas de serviço de sistema designadas. Tipicamente, o Firewall fecha essas portas de serviço do sistema, porque eles representam as fontes mais prováveis de insegurança do sistema. Para aceitar conexões de computadores remotos, no entanto, as portas de serviço do sistema devem ser abertas.

Esta lista mostra as portas padrão para serviços comuns.

- Portas 20-21 do FTP (Protocolo de Transferência de Arquivos)
- Mail Server (IMAP) Port 143
- Porta 110 do servidor de e-mail (POP3)
- Porta 25 do servidor de e-mail (SMTP)
- Microsoft Directory Server (MSFT DS) Port 445
- Porta 1433 do Microsoft SQL Server (MSFT SQL)
- Porta 3389 de Assistência remota / Servidor de terminal (RDP)
- Chamadas de procedimento remoto (RPC) Porta 135
- Porta 443 do servidor Web seguro (HTTPS)
- Porta 5000 de Plug and Play Universal (UPNP)
- Porta 80 do servidor Web (HTTP)
- Portas 137-139 do compartilhamento de arquivos do Windows (NETBIOS)

Neste capítulo

Configurando portas de serviço do sistema

Para permitir acesso remoto a um serviço em seu computador, você deve especificar o serviço e a porta correspondente que deve ser aberta. Somente selecione um serviço e uma porta se tiver certeza de que ela deva ser aberta. Muito raramente será necessário abrir uma porta.

Permitir acesso a uma porta de serviço do sistema existente

A partir do painel Serviços do sistema, é possível abrir ou fechar uma porta existente para permitir ou negar acesso remoto a um serviço de rede no computador. Uma porta de serviços do sistema aberta pode deixar seu computador vulnerável a ameaças à segurança vindas da Internet. Portanto, abra uma porta somente se necessário.

Para permitir o acesso a uma porta de serviço do sistema:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Serviços do sistema**.
3. Em **Abrir porta de serviço do sistema**, selecione um serviço do sistema para abrir uma porta.
4. Clique em **OK**.

Bloquear acesso a uma porta de serviço do sistema existente

A partir do painel Serviços do sistema, é possível abrir ou fechar uma porta existente para permitir ou negar acesso remoto a um serviço de rede no computador. Uma porta de serviços do sistema aberta pode deixar seu computador vulnerável a ameaças à segurança vindas da Internet. Portanto, abra uma porta somente se necessário.

Para bloquear o acesso a uma porta de serviço do sistema:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Serviços do sistema**.
3. Em **Abrir porta de serviço do sistema**, desmarque um serviço do sistema para fechar uma porta.
4. Clique em **OK**.

Configurar uma nova porta de serviço do sistema

A partir do painel Serviços do sistema, você pode adicionar uma nova porta de serviço do sistema que, por sua vez, pode ser aberta ou fechada para permitir ou negar acesso a um serviço de rede em seu computador. Uma porta de serviços do sistema aberta pode deixar seu computador vulnerável a ameaças à segurança vindas da Internet. Portanto, abra uma porta somente se necessário.

Para criar e configurar uma nova porta de serviço do sistema:

1 No painel Internet & Configuração de rede, clique em **Avançado**.
2 No painel Firewall, clique em **Serviços do sistema**.
3 Clique em **Adicionar**.
4 Em **Adicionar configuração de porta**, especifique o seguinte:
   - Nome do programa
   - Portas TCP/IP de entrada
   - Portas TCP/IP de saída
   - Portas UDP de entrada
   - Portas UDP de saída
5 Como opção, descreva a nova configuração.
6 Clique em **OK**.

   A nova porta de serviço do sistema configurada aparecerá em **Abrir porta de serviços do sistema**.

Modificar uma porta de serviço do sistema

Uma porta aberta e fechada permite e nega acesso a um serviço de rede em seu computador. A partir do painel Serviços do sistema, você pode modificar informações de entrada e de saída para uma porta existente. Se as informações da porta forem digitadas incorretamente, haverá falha no serviço do sistema.

Para modificar uma porta de serviço do sistema:

1 No painel Internet & Configuração de rede, clique em **Avançado**.
2 No painel Firewall, clique em **Serviços do sistema**.
3 Selecione um serviço do sistema e clique em **Editar**.
4 Em **Adicionar configuração de porta**, especifique o seguinte:
   - Nome do programa

- Portas TCP/IP de entrada
- Portas TCP/IP de saída
- Portas UDP de entrada
- Portas UDP de saída

5 Como opção, descreva a configuração modificada.

6 Clique em **OK**.

A porta de serviço do sistema com a configuração modificada aparecerá em **Abrir serviços do sistema**.

Remover uma porta de serviço do sistema

Uma porta aberta ou fechada permite ou nega acesso a um serviço de rede em seu computador. No painel Serviços do sistema, você pode remover uma porta existente e o serviço do sistema correspondente. Depois da remoção de uma porta e um serviço do sistema do painel Serviços do sistema, computadores remotos não podem mais acessar o serviço de rede em seu computador.

Para remover uma porta de serviço do sistema:

1 No painel Internet & Configuração de rede, clique em **Avançado**.

2 No painel Firewall, clique em **Serviços do sistema**.

3 Selecione um serviço do sistema e clique em **Remover**.

4 Na caixa de diálogo **Serviços do sistema**, clique em **Sim** para confirmar que deseja excluir o serviço do sistema.

A porta de serviço do sistema não aparecerá mais no painel Serviços do sistema.

CAPÍTULO 22

Gerenciando conexões do computador

Você pode configurar o Firewall para gerenciar conexões remotas específicas com o seu computador criando regras baseadas em endereços IP, que são associados a computadores remotos. Computadores associados a endereços IP confiáveis podem se conectar ao seu computador, e endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de se conectarem ao seu computador.

O Ao permitir uma conexão, verifique se o computador em que está confiando é seguro. Se um computador no qual você confia for infectado por um worm ou outro mecanismo, você estará vulnerável à infecção. Além disso, a McAfee recomenda que os computadores confiáveis também sejam protegidos por um firewall e um programa antivírus atualizado. Firewall não registra tráfego nem gera alertas de eventos de endereços IP contidos na lista Endereços IP confiáveis.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Neste capítulo

Confiando em conexões de computador

Você pode adicionar, editar e remover endereços IP confiáveis no painel IPs confiáveis e proibidos, em **Endereços IP confiáveis**.

A lista **Endereços IP confiáveis**, no painel IPs confiáveis e proibidos, possibilita permitir que todo o tráfego proveniente de um computador atinja o seu computador. O Firewall não registra tráfego nem gera alertas de eventos de endereços IP contidos na lista **Endereços IP confiáveis**.

O Firewall confia em todos os endereços IP selecionados da lista e sempre permite o tráfego de um IP confiável através do firewall em qualquer porta. O Firewall não registra nenhum evento dos endereços IP confiáveis. Atividades entre um computador associado a um endereço IP confiável e o seu próprio computador não são filtradas nem analisadas pelo Firewall.

Ao permitir uma conexão, verifique se o computador em que está confiando é seguro. Se um computador no qual você confia for infectado por um worm ou outro mecanismo, você estará vulnerável à infecção. Além disso, a McAfee recomenda que os computadores confiáveis também sejam protegidos por um firewall e um programa antivírus atualizado.

Adicionar uma conexão de computador confiável

Você pode usar o Firewall para adicionar uma conexão de computador confiável e o endereço IP associado.

A lista **Endereços IP confiáveis**, no painel IPs confiáveis e proibidos, possibilita permitir que todo o tráfego proveniente de um computador atinja o seu computador. O Firewall não registra tráfego nem gera alertas de eventos de endereços IP contidos na lista **Endereços IP confiáveis**.

Computadores associados a endereços IP confiáveis podem sempre se conectar ao seu computador. Antes de adicionar, editar ou remover um endereço IP confiável, verifique se ele é seguro para comunicação ou remoção.

Para adicionar uma conexão de computador confiável:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **IPs confiáveis e proibidos**.
3. No painel IPs confiáveis e proibidos, selecione **Endereços IP confiáveis**.
4. Clique em **Adicionar**.
5. Em **Adicionar regra de endereço IP confiável**, execute um dos procedimentos a seguir:
   - Selecione um **Endereço IP único** e, em seguida, digite o endereço IP.
   - Selecione um **Intervalo de endereços IP** e, em seguida, digite os endereços IP inicial e final nas caixas **Do endereço IP** e **Ao endereço IP**.
6. Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.
7. Como opção, digite uma descrição para a regra.
8. Clique em **OK**.
9. Na caixa de diálogo Adicionar regra de endereço IP confiável, clique em **Sim** para confirmar que você deseja adicionar a conexão de computador confiável.

   O endereço IP adicionado é exibido em **Endereços IP confiáveis**.

Adicionar um computador confiável a partir do registro de Eventos de entrada

Você pode adicionar uma conexão de computador confiável e seu endereço IP correspondente, a partir do registro de Eventos de entrada.

Computadores associados a endereços IP confiáveis podem sempre se conectar ao seu computador. Antes de adicionar, editar ou remover um endereço IP confiável, verifique se ele é seguro para comunicação ou remoção.

Para adicionar um computador confiável a partir do registro de Eventos de entrada:

1. Assegure-se de que o menu Avançado esteja ativado. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Clique em **Internet e rede** e então em **Eventos de entrada**.
4. No painel Eventos de entrada, selecione um endereço IP de origem e clique em **Confiar neste endereço**.
5. Na caixa de diálogo Adicionar regra de endereço IP confiável, clique em **Sim** para confirmar que você deseja confiar no endereço IP.

   O endereço IP adicionado é exibido em **Endereços IP confiáveis**.

Tópicos relacionados

- Registro de eventos (página 170)

Editar uma conexão de computador confiável

Você pode usar o Firewall para editar uma conexão de computador confiável e o endereço IP associado.

Computadores associados a endereços IP confiáveis podem sempre se conectar ao seu computador. Antes de adicionar, editar ou remover um endereço IP confiável, verifique se ele é seguro para comunicação ou remoção.

Para editar uma conexão de computador confiável:

1 No painel Internet & Configuração de rede, clique em **Avançado**.
2 No painel Firewall, clique em **IPs confiáveis e proibidos**.
3 No painel IPs confiáveis e proibidos, selecione **Endereços IP confiáveis**.
4 Selecione um endereço IP e clique em **Editar**.
5 Em **Adicionar regra de endereço IP confiável**, execute um dos procedimentos a seguir:
   - Selecione um **Endereço IP único** e, em seguida, digite o endereço IP.
   - Selecione um **Intervalo de endereços IP** e, em seguida, digite os endereços IP inicial e final nas caixas **Do endereço IP** e **Ao endereço IP**.
6 Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.
7 Como opção, digite uma descrição para a regra.
8 Clique em **OK**.

   O endereço IP modificado é exibido em **Endereços IP confiáveis**.

Remover uma conexão de computador confiável

Você pode usar o Firewall para remover uma conexão de computador confiável e o endereço IP associado.

Computadores associados a endereços IP confiáveis podem sempre se conectar ao seu computador. Antes de adicionar, editar ou remover um endereço IP confiável, verifique se ele é seguro para comunicação ou remoção.

Para remover uma conexão de computador confiável:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **IPs confiáveis e proibidos**.
3. No painel IPs confiáveis e proibidos, selecione **Endereços IP confiáveis**.
4. Selecione um endereço IP e clique em **Remover**.
5. Na caixa de diálogo **IPs confiáveis e proibidos**, clique em **Sim** para confirmar que deseja remover o endereço IP confiável, em **Endereços IP confiáveis**.

Proibindo conexões de computador

Você pode adicionar, editar e remover endereços IP confiáveis no painel IPs confiáveis e proibidos, em **Endereços IP proibidos**.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Adicionar uma conexão de computador proibida

Você pode usar o Firewall para adicionar uma conexão de computador proibida e o endereço IP associado.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Para adicionar uma conexão de computador proibida:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **IPs confiáveis e proibidos**.
3. No painel IPs confiáveis e proibidos, selecione **Endereços IP proibidos**.
4. Clique em **Adicionar**.
5. Em Adicionar regra de endereço IP proibido, execute um dos procedimentos a seguir:
   - Selecione um **Endereço IP único** e, em seguida, digite o endereço IP.

- Selecione um **Intervalo de endereços IP** e, em seguida, digite os endereços IP inicial e final nos campos **Do endereço IP** e **Ao endereço IP**.

6 Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.

7 Você também pode digitar uma descrição para a regra.

8 Clique em **OK**.

9 Na caixa de diálogo **Adicionar regra de endereço IP proibido**, clique em **Sim** para confirmar que você deseja adicionar a conexão de computador proibida.

   O endereço IP adicionado é exibido em **Endereços IP proibidos**.

Editar uma conexão de computador proibida

Você pode usar o Firewall para editar uma conexão de computador proibida e o endereço IP associado.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Para editar uma conexão de computador proibida:

1 No painel Internet & Configuração de rede, clique em **Avançado**.

2 No painel Firewall, clique em **IPs confiáveis e proibidos**.

3 No painel IPs confiáveis e proibidos, selecione **Endereços IP proibidos**.

4 Selecione um endereço IP e clique em **Editar**.

5 Em **Adicionar regra de endereço IP confiável**, execute um dos procedimentos a seguir:

   - Selecione um **Endereço IP único** e, em seguida, digite o endereço IP.
   - Selecione um **Intervalo de endereços IP** e digite os endereços IP inicial e final nos campos **Do endereço IP** e **Ao endereço IP**.

6 Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.

7 Você pode, também, digitar uma descrição para a regra.

Clique em **OK**. O endereço IP modificado é exibido em **Endereços IP proibidos**.

Remover uma conexão de computador proibida

Você pode usar o Firewall para remover uma conexão de computador proibida e o endereço IP associado.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Para remover uma conexão de computador proibida:

1 No painel Internet & Configuração de rede, clique em **Avançado**.

2 No painel Firewall, clique em **IPs confiáveis e proibidos**.

3 No painel IPs confiáveis e proibidos, selecione **Endereços IP proibidos**.

4 Selecione um endereço IP e clique em **Remover**.

5 Na caixa de diálogo **IPs confiáveis e proibidos**, clique em **Sim** para confirmar que deseja remover o endereço IP confiável dos **Endereços IP proibidos**.

Proibir um computador a partir do registro de Eventos de entrada

Você pode proibir uma conexão de computador confiável e seu endereço IP correspondente, a partir do registro de Eventos de entrada.

Endereços IP que aparecem no registro de Eventos de entrada são bloqueados. Portanto, a proibição de um endereço não acrescenta nenhuma proteção adicional, a não ser que seu computador utilize portas que são deliberadamente abertas ou inclua um programa ao qual o acesso à Internet tenha sido concedido.

Adicione um endereço IP à lista **Endereços IP proibidos** somente se houver uma ou mais portas deliberadamente abertas e se houver necessidade de bloquear o acesso desse endereço às portas abertas.

É possível usar a página Eventos de entrada, que lista os endereços IP de todo o tráfego da Internet, para proibir um endereço IP suspeito de ser a origem de atividade suspeita ou não desejada na Internet.

Para proibir uma conexão de computador confiável a partir do registro de Eventos de entrada:

1. Assegure-se de que o menu Avançado esteja ativado. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Clique em **Internet e rede** e então em **Eventos de entrada**.
4. No painel Eventos de entrada, selecione um endereço IP de origem e clique em **Proibir este endereço**.
5. Na caixa de diálogo **Adicionar regra de endereço IP proibido**, clique em **Sim** para confirmar que você deseja proibir o endereço IP.

   O endereço IP adicionado é exibido em **Endereços IP proibidos**.

Tópicos relacionados

- Registro de eventos (página 170)

Proibir um computador a partir do registro de Eventos de detecção de invasão

Você pode proibir uma conexão de computador confiável e seu endereço IP correspondente, a partir do registro de Eventos detecção de invasão.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Para proibir uma conexão de computador a partir do registro de Eventos de detecção de invasão:

1. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Clique em **Internet & rede** e, em seguida, clique em **Eventos de detecção de invasão**.
4. No painel Eventos de detecção de invasão, selecione um endereço IP de origem e clique em **Proibir este endereço**.
5. Na caixa de diálogo **Adicionar regra de endereço IP proibido**, clique em **Sim** para confirmar que você deseja proibir o endereço IP.

   O endereço IP adicionado é exibido em **Endereços IP proibidos**.

Tópicos relacionados

- Registro de eventos (página 170)

CAPÍTULO 23

Registro, monitoramento e análise

O Firewall fornece análise, registros e monitoramento amplos e de fácil leitura para eventos e tráfego da Internet. Noções básicas sobre tráfego e eventos da Internet ajudam você a gerenciar suas conexões com a Internet.

Neste capítulo

Registro de eventos

O Firewall permite que você especifique se deseja ativar ou desativar o registro e, se ativado, que tipo de eventos registrar. O registro de eventos permite que você verifique eventos recentes de entrada e de saída. Também é possível exibir eventos de detecção de invasões.

Configurar registro de eventos

Para rastrear eventos e atividades do firewall, você pode especificar e configurar os tipos de eventos a serem exibidos.

Para configurar o registro de eventos:

1. No painel Internet & Configuração de rede, clique em **Avançado**.
2. No painel Firewall, clique em **Configurações do registro de eventos**.
3. No painel Configurações do registro de eventos, execute um dos procedimentos a seguir:
   - Selecione **Registrar evento**, para ativar o registro do evento.
   - Selecione **Não registrar evento**, para desativar o registro do evento.
4. Em **Configurações do registro de eventos**, especifique quais tipos de eventos registrar. Os tipos de eventos incluem o seguinte:
   - Pings ICMP
   - Tráfego de endereços IP proibidos
   - Eventos nas portas de serviço do sistema
   - Eventos em portas desconhecidas
   - Eventos da detecção de invasão (IDS)
5. Para impedir o registro em portas específicas, selecione **Não registrar eventos nas seguintes portas**, e digite números de porta únicos separados por vírgulas ou intervalos de portas separados por traços. Por exemplo, `137-139, 445, 400-5000`.
6. Clique em **OK**.

Exibir eventos recentes

Se o registro estiver ativado, você poderá exibir os eventos recentes. O painel Eventos recentes exibe a data e a descrição do evento. Ele exibe apenas as atividades de programas cujo acesso à Internet foi expressamente bloqueado.

Para exibir os eventos recentes do Firewall:

- No **Menu Avançado**, no painel Tarefas comuns, clique em **Registros & relatórios** ou em **Exibir eventos recentes**. Uma alternativa é clicar em **Exibir eventos recentes** no painel Tarefas comuns do Menu básico.

Exibir eventos de entrada

Se o registro estiver ativado, é possível exibir e classificar os eventos de entrada.

O registro de Eventos de entrada inclui as seguintes categorias de registro:

- Data e hora
- Endereço IP de origem
- Nome do host
- Tipo de evento e informação

Para exibir os eventos de entrada do firewall:

1. Assegure-se de que o menu Avançado esteja ativado. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Clique em **Internet e rede** e então em **Eventos de entrada**.

Observação: Você pode confiar, proibir e rastrear um endereço IP a partir do registro de Eventos de entrada.

Tópicos relacionados

- Adicionar um computador confiável a partir do registro de Eventos de entrada (página 160)
- Proibir um computador a partir do registro de Eventos de entrada (página 166)
- Rastrear um computador a partir do registro de Eventos de entrada (página 175)

Exibir eventos de saída

Se o registro estiver ativado, é possível exibir os eventos de saída. Eventos de saída incluem o nome do programa que tenta acesso de saída, data e hora do evento e local do programa em seu computador.

Para exibir os eventos de saída do firewall:

1. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Selecione **Internet e rede** e em **Eventos de saída**.

Observação: Você pode conceder acesso total e apenas de saída para um programa a partir do registro de Eventos de saída. Também é possível localizar informações adicionais sobre o programa.

Tópicos relacionados

- Conceder acesso total a partir do registro de Eventos de saída (página 144)
- Conceder somente acesso de saída a partir do registro de Eventos de saída (página 146)
- Obter informações do programa a partir do registro de Eventos de saída (página 151)

Exibir eventos de detecção de invasão

Se o registro estiver ativado, é possível exibir os eventos de entrada. Os eventos de Detecção de invasão exibem a data e hora, o IP de origem e o nome do host do evento. O registro também descreve o tipo de evento.

Para exibir eventos de detecção de invasão:

1. No painel Tarefas comuns, clique em **Registros & relatórios**.
2. Em Eventos recentes, clique em **Exibir registro**.
3. Clique em **Internet & rede** e, em seguida, clique em **Eventos de detecção de invasão**.

Observação: Você pode proibir e rastrear um endereço IP a partir do registro de Eventos de detecção de invasão.

Tópicos relacionados

- Proibir um computador a partir do registro de Eventos de detecção de invasão (página 167)
- Rastrear um computador a partir do registro de Eventos de detecção de invasão (página 176)

Trabalhando com estatísticas

O Firewall aproveita o site de segurança Hackerwatch da McAfee para fornecer estatísticas sobre eventos de segurança e atividades de porta globais da Internet.

Exibir estatística global dos eventos de segurança

O HackerWatch rastreia mundialmente eventos de segurança na Internet, e você pode exibi-los no SecurityCenter. As informações rastreadas listam os incidentes relatados ao HackerWatch nas últimas 24 horas, 7 dias, e 30 dias.

Para exibir estatísticas globais de segurança:

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Hackerwatch**.
3. Exiba as estatísticas de eventos de segurança em **Rastreamento de eventos**.

Exibir a atividade global de portas da Internet

O HackerWatch rastreia mundialmente eventos de segurança na Internet, e você pode exibi-los no SecurityCenter. As informações exibidas incluem os principais eventos de portas relatados ao HackerWatch durante os últimos sete dias. Normalmente, são exibidas informações de portas HTTP, TCP e UDP.

Para exibir atividades de portas em todo o mundo:

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Hackerwatch**.
3. Exiba os principais eventos de portas em **Atividade recente de porta**.

Rastreando tráfego da Internet

O Firewall oferece várias opções para rastrear o tráfego da Internet. Essas opções permitem que você rastreie geograficamente um computador da rede, obtenha informações de domínio e rede e rastreie computadores dos registros de Eventos de entrada e Eventos de detecção de invasão.

Rastrear geograficamente um computador da rede

Você pode usar o Rastreador visual para localizar geograficamente um computador que esteja se conectando ou tentando se conectar ao seu computador, usando o nome ou endereço IP dele. Também é possível acessar informações de rede e de inscrição com o Rastreador visual. O Rastreador visual exibe um mapa-múndi com a rota mais provável pela qual os dados estão trafegando entre o computador de origem e o seu computador.

Para localizar geograficamente um computador:

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Rastreador visual**.
3. Digite o endereço IP do computador e clique em **Rastrear**.
4. Em **Rastreador visual**, selecione **Exibir mapa**.

Observação: Não é possível rastrear eventos de endereços IP em looping, privados ou inválidos.

Obter informações sobre a inscrição de um computador

Você pode obter as informações de inscrição de um computador no SecurityCenter, usando o Rastreador Visual. As informações incluem o nome de domínio, o nome e endereço do inscrito e o contato administrativo.

Para obter as informações de domínio de um computador:

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Rastreador visual**.
3. Digite o endereço IP do computador e clique em **Rastrear**.
4. Em **Rastreador visual**, selecione **Exibir inscrito**.

Obter informações de rede de um computador

Você pode obter as informações de rede de um computador no SecurityCenter, usando o Rastreador Visual. As informações de rede incluem detalhes sobre a rede em que o domínio reside.

Para obter as informações de rede de um computador:

1 Verifique se o Menu avançado está ativado e clique em **Ferramentas**.

2 No painel Ferramentas, clique em **Rastreador visual**.

3 Digite o endereço IP do computador e clique em **Rastrear**.

4 Em **Rastreador visual**, selecione **Exibir rede**.

Rastrear um computador a partir do registro de Eventos de entrada

No painel Eventos de entrada, você pode rastrear um endereço IP que aparece no registro de Eventos de entrada.

Para rastrear um computador a partir do registro de Eventos de entrada:

1 Assegure-se de que o menu Avançado esteja ativado. No painel Tarefas comuns, clique em **Relatórios e registros**.

2 Em **Eventos recentes**, clique em **Exibir registro**.

3 Clique em **Internet e rede** e então em **Eventos de entrada**.

4 No painel Eventos de entrada, selecione um endereço IP de origem e clique em **Rastrear este endereço**.

5 No painel do Rastreador visual, clique em umas destas opções:

   - **Exibir mapa**: Localizar geograficamente um computador, usando o endereço IP selecionado.
   - **Exibição inscrito**: Localizar informações de domínio usando o endereço IP selecionado.
   - **Exibição da rede**: Localizar informações de rede usando o endereço IP selecionado.

6 Clique em **Concluído**.

Tópicos relacionados

- Rastreando tráfego da Internet (página 174)
- Exibir eventos de entrada (página 171)

Rastrear um computador a partir do registro de Eventos de detecção de invasão

No painel Eventos de detecção de invasão, você pode rastrear um endereço IP que aparece no registro de Eventos de detecção de invasão.

Para rastrear um computador a partir do registro de Eventos de detecção de invasão:

1 No painel Tarefas comuns, clique em **Relatórios e registros**.

2 Em **Eventos recentes**, clique em **Exibir registro**.

3 Clique em **Internet & rede** e, em seguida, clique em **Eventos de detecção de invasão**. No painel Eventos de detecção de invasão, selecione um endereço IP de origem e clique em **Rastrear este endereço**.

4 No painel do Rastreador visual, clique em umas destas opções:

   - **Exibir mapa**: Localizar geograficamente um computador, usando o endereço IP selecionado.
   - **Exibição do inscrito**: Localizar informações de domínio, usando o endereço IP selecionado.
   - **Exibição da rede**: Localizar informações de rede, usando o endereço IP selecionado.

5 Clique em **Concluído**.

Tópicos relacionados

- Rastreando tráfego da Internet (página 174)
- Registro, monitoramento e análise (página 169)

Rastrear um endereço IP monitorado

É possível rastrear um endereço IP monitorado, para obter uma exibição geográfica que mostre a rota mais provável dos dados, do computador de origem até o seu. Além disso, você pode obter informações de inscrição e de rede sobre o endereço IP.

Para monitorar o uso de largura de banda pelos programas:

1 Verifique se o Menu avançado está ativado e clique em **Ferramentas**.

2 No painel Ferramentas, clique em **Monitor de tráfego**.

3 Em **Monitor de tráfego**, clique em **Programas ativos**.

4 Selecione um programa e o endereço IP que aparece abaixo do nome do programa.

5 Em **Atividade do programa**, clique em **Rastrear este IP**.

6 Em **Rastreador visual**, você pode ver um mapa que exibe a rota mais provável pela qual os dados estão trafegando entre o computador de origem e o seu computador. Além disso, você pode obter informações de inscrição e de rede sobre o endereço IP.

Observação: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Rastreador visual**.

Tópicos relacionados

- Monitorando tráfego da Internet (página 178)

Monitorando tráfego da Internet

O Firewall fornece vários métodos para monitorar seu tráfego da Internet, inclusive os seguintes:

- **Gráfico de análise do tráfego**: Exibe tráfego recente de entrada e saída da Internet.
- **Gráfico de utilização do tráfego**: Exibe a porcentagem da largura de banda usada pelos programas mais ativos nas últimas 24 horas.
- **Programas ativos**: Exibe os programas que atualmente usam o maior número de conexões de rede em seu computador e quais endereços IP são acessados pelos programas.

Sobre o Gráfico de análise de tráfego

O gráfico de Análise de tráfego é uma representação numérica e gráfica do tráfego de entrada e saída da Internet. Ele também mostra quais programas estão usando o maior número de conexões de rede em seu computador e os endereços IP que o programa acessa.

No painel Análise de tráfego, é possível exibir tráfego recente de entrada e saída na Internet e taxas de transferência atuais, médias e máximas. Você também pode exibir o volume de tráfego, inclusive a quantidade de tráfego desde que o firewall foi iniciado, além do tráfego total do mês corrente e dos meses anteriores.

O painel Análise de tráfego exibe a atividade de Internet do computador em tempo real, incluindo o volume e taxa de tráfego recente de entrada e saída de Internet, velocidade da conexão e total de bytes transferidos pela Internet.

A linha verde sólida representa a taxa atual de transferência do tráfego de entrada. A linha verde pontilhada representa a taxa média de transferência do tráfego de entrada. Se a taxa atual de transferência e a taxa média de transferência forem iguais, a linha pontilhada não será exibida no gráfico. A linha sólida representará duas taxas de transferência: a média e a atual.

A linha vermelha sólida representa a taxa atual de transferência do tráfego de saída. A linha vermelha pontilhada representa a taxa média de transferência do tráfego de saída. Se a taxa atual de transferência e a taxa média de transferência forem iguais, a linha pontilhada não será exibida no gráfico. A linha sólida representará duas taxas de transferência: a média e a atual.

Tópicos relacionados

- Analisar tráfego de entrada e de saída (página 179)

Analisar tráfego de entrada e de saída

O gráfico de Análise de tráfego é uma representação numérica e gráfica do tráfego de entrada e saída da Internet. Ele também mostra quais programas estão usando o maior número de conexões de rede em seu computador e os endereços IP que o programa acessa.

Para analisar tráfego de entrada e de saída:

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de tráfego**.
3. Em **Monitor de tráfego**, clique em **Análise de tráfego**.

Dica: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Análise de tráfego**.

Tópicos relacionados

- Sobre o Gráfico de análise de tráfego (página 178)

Monitorar largura de banda de um programa

Você pode visualizar um gráfico de torta, que exibe a porcentagem aproximada de largura de banda usada pelos programas mais ativos em seu computador durante as últimas vinte e quatro horas. O gráfico oferece uma representação visual das quantidades relativas de largura de banda usada pelos programas.

Para monitorar o uso de largura de banda pelos programas:

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de tráfego**.
3. Em **Monitor de tráfego**, clique em **Utilização de tráfego**.

Dica: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Utilização de tráfego**.

Monitorar a atividade de um programa

Você pode exibir a atividade de entrada e saída dos programas, que exibe conexões e portas de computadores remotos.

Para monitorar o uso de largura de banda pelos programas:

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de tráfego**.
3. Em **Monitor de tráfego**, clique em **Programas ativos**.
4. Você pode exibir as seguintes informações:
   - Gráfico de atividades do programa: Selecione um programa para exibir um gráfico de suas atividades.
   - Conexão de escuta: Selecione um item de Escuta sob o nome do programa.
   - Conexão do computador: Selecione um endereço IP sob o nome do programa, serviço ou processo do sistema.

Observação: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Programas ativos**.

CAPÍTULO 24

Saiba mais sobre segurança da Internet

O Firewall utiliza o site de segurança da McAfee, Hackerwatch, para fornecer informações atualizadas sobre programas e atividade global da Internet. O Hackerwatch também fornece um tutorial em HTML sobre o Firewall.

Neste capítulo

Iniciar o tutorial do Hackerwatch

Para aprender sobre o Firewall, você pode acessar o tutorial do Hackerwatch a partir do SecurityCenter.

Para iniciar o tutorial do Hackerwatch:

1 Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2 No painel Ferramentas, clique em **Hackerwatch**.
3 Em **Recursos do Hackerwatch**, clique em **Exibir tutorial**.

CAPÍTULO 25

McAfee SpamKiller

O SpamKiller filtra mensagens de e-mail com spam e phishing e oferece o seguinte.

Opções do usuário

- Filtrar várias contas de e-mail
- Importar contatos para a lista de Amigos
- Criar filtros personalizados e relatar o spam à McAfee para análise
- Opções para marcar como spam e marcar como não spam
- Suporte para vários usuários (Windows® XP e Vista™)

Filtragem

- Atualizar filtros automaticamente
- Criar filtros de mensagens de e-mail personalizados
- Mecanismo de filtragem central em várias camadas
- Filtros phishing

Neste capítulo

Recursos

Esta versão do SpamKiller oferece os seguintes recursos.

Filtragem

A tecnologia de filtragem avançada aprimora a sua experiência de usuário.

Phishing

O recurso phishing identifica e bloqueia facilmente os sites da Web de phishing em potencial.

Instalação

Instalação e configuração otimizadas.

Interface

Interface de usuário intuitiva para manter o computador livre de spam.

Suporte

Suporte técnico gratuito por meio de mensagens instantâneas e e-mail para oferecer um atendimento ao cliente fácil, imediato e em tempo real.

Processamento de mensagens de spam

Configurações opcionais para manipulação das mensagens de e-mail de spam. Isso permite exibir mensagens que podem ter sido filtradas incorretamente.

Programas de e-mail suportados

- Todos os programas de e-mail POP3
- Suporte MAPI para Outlook® 2000 ou posterior
- Suporte ao filtro de Web mail com POP3 ou MSN®/Hotmail® pago

Barras de ferramentas de e-mail suportadas

- Outlook Express 6.0 ou superior
- Outlook 2000, XP, 2003 ou 2007
- Eudora® 6.0 ou posterior
- Thunderbird™ 1.5 ou posterior

Proteção contra phishing suportada

Qualquer navegador da Web compatível com HTTP, incluindo:

- Internet Explorer
- Firefox®
- Netscape®

CAPÍTULO 26

Gerenciando contas de Web mail

Você pode adicionar contas de Web mail à filtragem de spam, editar informações de contas de Web mail ou remover as contas de Web mail quando não desejar mais filtrá-las.

Você também pode gerenciar a filtragem de Web mail. Por exemplo, você pode desativar ou ativar a filtragem de mensagens de e-mail em suas contas de Web mail, gerenciar as mensagens que foram filtradas e exibir os registros.

Neste capítulo

Adicionando contas de Web mail

Você pode adicionar os seguintes tipos de contas de Web mail para que possam ser filtradas em busca de spam.

- Web mail POP3 (por exemplo, Yahoo ∃)
- MSN/Hotmail (somente as versões pagas são totalmente suportadas)

Adicionar uma conta de Web mail POP3 ou MSN/Hotmail

Adicione uma conta de e-mail para ser filtrada em busca de spam.

Para adicionar uma conta de Web mail POP3 ou MSN/Hotmail:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Contas de Web mail**.

5 No painel Contas de Web mail, clique em **Adicionar**.

6 Especifique as informações sobre a conta de Web mail nas seguintes caixas:

   - **Descrição**: Descreve a conta. Digite qualquer informação nessa caixa.
   - **Endereço de e-mail**: Especifica o endereço de e-mail dessa conta.
   - **Tipo de conta**: Especifica o tipo de conta de e-mail
   - **Servidor**: Especifica o nome do servidor dessa conta.
   - **Nome do usuário**: Especifica o nome do usuário dessa conta
   - **Senha**: Especifica a senha usada para acessar essa conta.
   - **Confirmar senha**: Confirma a senha.

7 Clique em **Avançar**.

8 Em **Opções de verificação**, execute uma das ações a seguir para determinar quando o SpamKiller verificará sua conta em busca de spam:

   - Digite um valor na caixa **Verificar a cada**.

O SpamKiller verifica essa conta no intervalo (número de minutos) que você especificar. Se você digitar o número zero, o SpamKiller verificará a conta apenas ao se conectar.

- Selecione a caixa de seleção **Verificar ao iniciar**.

  O SpamKiller verifica a conta sempre que o computador é reiniciado. Use essa opção se possuir uma conexão direta.

9 Se você estiver usando uma conexão discada, execute uma das seguintes ações em **Opções de conexão** para determinar como o SpamKiller se conectará à Internet:

- Clique em **Nunca discar uma conexão.**

  O SpamKiller não disca automaticamente uma conexão para você. É necessário iniciar manualmente a conexão discada.

- Clique em **Discar quando não houver conexão disponível**.

  Quando uma conexão com a Internet não estiver disponível, o SpamKiller tentará se conectar usando a conexão discada que você especificar.

- Clique em **Discar sempre para a conexão especificada**.

  O SpamKiller tentará se conectar usando a conexão discada que você especificou.

- Clique em uma entrada na lista **Discar esta conexão**.

  Essa entrada especifica a conexão discada à qual o SpamKiller tenta se conectar.

- Clique na caixa de seleção **Permanecer conectado depois que a filtragem for concluída**.

  Seu computador permanecerá conectado à Internet depois que a filtragem for concluída.

10 Clique em **Concluir**.

Modificando contas de Web mail

Você pode ativar ou desativar contas de Web mail ou editar as suas informações. Por exemplo, você pode alterar o endereço de e-mail, a descrição da conta, o tipo de conta, a senha e a freqüência com que o SpamKiller verifica se há spam na conta e como o computador se conecta à Internet.

Editar uma conta de Web mail POP3 ou MSN/Hotmail

Você pode ativar ou desativar contas de Web mail ou editar as suas informações. Por exemplo, altere o endereço de e-mail, a descrição da conta, as informações do servidor, a freqüência com que o SpamKiller verifica se há spam na conta e como o computador se conecta à Internet.

Para modificar uma conta de Web mail POP3 ou MSN/Hotmail:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Contas de Web mail**.

5 Selecione a conta que você deseja modificar e, em seguida, clique em **Editar**.

6 Edite as informações da conta nas seguintes caixas:

- **Descrição**: Descreve a conta. Digite qualquer informação nessa caixa.
- **Endereço de e-mail**: Especifica o endereço de e-mail dessa conta.
- **Tipo de conta**: Especifica o tipo de conta de e-mail
- **Servidor**: Especifica o nome do servidor dessa conta.
- **Nome do usuário**: Especifica o nome do usuário dessa conta
- **Senha**: Especifica a senha usada para acessar essa conta.
- **Confirmar senha**: Confirma a senha.

7 Clique em **Avançar**.

8 Em **Opções de verificação**, execute uma das ações a seguir para determinar quando o SpamKiller verificará sua conta em busca de spam:

- Digite um valor na caixa **Verificar a cada**.

O SpamKiller verifica essa conta no intervalo (número de minutos) que você especificar. Se você digitar o número zero, o SpamKiller verificará a conta apenas ao se conectar.

- Selecione a caixa de seleção **Verificar ao iniciar**.

  O SpamKiller verifica a conta sempre que o computador é reiniciado. Use essa opção se possuir uma conexão direta.

9 Se você estiver usando uma conexão discada, execute uma das seguintes ações em **Opções de conexão** para determinar como o SpamKiller se conectará à Internet:

- Clique em **Nunca discar uma conexão.**

  O SpamKiller não disca automaticamente uma conexão para você. É necessário iniciar manualmente a conexão discada.

- Clique em **Discar quando não houver conexão disponível**.

  Quando uma conexão com a Internet não estiver disponível, o SpamKiller tentará se conectar usando a conexão discada que você especificar.

- Clique em **Discar sempre para a conexão especificada**.

  O SpamKiller tentará se conectar usando a conexão discada que você especificou.

- Clique em uma entrada na lista **Discar esta conexão**.

  Essa entrada especifica a conexão discada à qual o SpamKiller tenta se conectar.

- Clique na caixa de seleção **Permanecer conectado depois que a filtragem for concluída**.

  Seu computador permanecerá conectado à Internet depois que a filtragem for concluída.

10 Clique em **Concluir**.

Removendo contas de Web mail

Você pode remover as contas de Web mail que não deseja mais filtrar.

Remover contas de Web mail

Remova uma conta de e-mail se não deseja mais que ela seja filtrada.

Para remover contas de Web mail:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Contas de Web mail**.
5. Selecione a conta a ser removida e clique em **Remover**.

Gerenciando a filtragem de Web mail

Você pode desativar ou ativar a filtragem de mensagens de e-mail em suas contas de Web mail, gerenciar as mensagens que foram filtradas e exibir os registros.

Desativar filtragem de Web mail

Você pode desativar a filtragem de Web mail e impedir que mensagens de e-mail sejam filtradas.

Para desativar a filtragem de Web mail:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Contas de Web mail**.
5. Desmarque a caixa de seleção ao lado da conta que você deseja desativar.
6. Clique em **OK**.

Ativar filtragem de Web mail

Se você desativou alguma conta de Web mail, poderá ativá-la novamente.

Para ativar a filtragem de Web mail:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Contas de Web mail**.
5. Marque a caixa de seleção ao lado da conta que você deseja ativar.
6. Clique em **OK**.

Gerenciar mensagens filtradas nas contas de Web mail

Você pode exibir, copiar ou excluir mensagens que foram filtradas em sua conta de Web mail.

Para exibir, copiar ou excluir as mensagens filtradas da sua conta de Web mail:

1. No Menu avançado, clique em **Relatórios e registros**.
2. No painel Relatórios e registros, clique em **Web mail filtrado**.
3. No painel Web mail filtrado, selecione a mensagem que você deseja exibir, copiar ou excluir.
4. Em **Desejo**, execute uma das seguintes ações:
   - Clique em **Copiar** para copiar a mensagem para a área de transferência.
   - Clique em **Excluir** para excluir a mensagem.

Exibir registros do Web mail filtrado

Você pode exibir os registros do Web mail filtrado. Por exemplo, você pode saber quando a mensagem de e-mail foi filtrada e a conta que a recebeu.

Para exibir registros do Web mail filtrado:

1. No Menu avançado, clique em **Relatórios e registros**.
2. No painel Relatórios e registros, clique em **Eventos recentes**.
3. No painel Eventos recentes, clique em **Exibir registro**.
4. No painel esquerdo, expanda a lista **E-mail e mensagens instantâneas** e, em seguida, clique em **Eventos de filtragem de Web mail**.
5. Selecione o registro que você deseja exibir.
6. Em **Detalhes**, exiba as informações sobre o registro.

CAPÍTULO 27

Gerenciando amigos

Para garantir o recebimento de todas as mensagens de seus amigos, adicione os respectivos endereços à sua lista de amigos. Você também pode adicionar domínios, editar ou remover amigos e programar atualizações automáticas da sua lista de amigos.

Neste capítulo

Noções básicas sobre como gerenciar os amigos

Esta seção descreve como gerenciar os amigos.

Adicionar manualmente os amigos a partir da barra de ferramentas do SpamKiller

Para garantir o recebimento de todas as mensagens de seus amigos, adicione os respectivos endereços à sua lista de amigos.

Se estiver usando os programas de e-mail Outlook, Outlook Express, Windows Mail, Eudora ou Thunderbird, você poderá adicionar amigos usando a barra de ferramentas do SpamKiller.

Para adicionar um amigo no Outlook:

- No seu programa de e-mail, selecione uma mensagem e, em seguida, clique em **Adicionar amigo**.

Para adicionar um amigo no Outlook Express, no Windows Mail no Eudora ou no Thunderbird:

- No seu programa de e-mail, selecione uma mensagem. Em seguida, no menu **SpamKiller**, clique em **Adicionar amigo**.

Adicionar amigos manualmente

Para garantir o recebimento de todas as mensagens de seus amigos, adicione os respectivos endereços à sua lista de amigos. Você também pode adicionar domínios.

Para adicionar amigos manualmente:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em Proteção contra spam, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Amigos**.
5. No painel Amigos, clique em **Adicionar**.
6. Digite as informações de seu amigo nas seguintes caixas:
   - **Nome**: Especifica o nome do seu amigo.
   - **Tipo**: Indica se você está especificando um único endereço de e-mail ou um domínio inteiro.
   - **Endereço de e-mail**: Especifica o endereço de e-mail do seu amigo ou o domínio que você não deseja filtrar.
7. Clique em **OK**.

Editar amigos

Se as informações de um amigo forem alteradas, você poderá atualizar a lista para garantir que receberá todas as mensagens dele.

Para editar amigos:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em Proteção contra spam, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Amigos**.

5 Selecione o amigo que você deseja editar e, em seguida, clique em **Editar**.

6 Edite as informações de seu amigo nas seguintes caixas:

- **Nome**: Especifica o nome do seu amigo.
- **Tipo**: Especifica se você está editando um único endereço de e-mail ou um domínio inteiro.
- **Endereço de e-mail**: Especifica o endereço de e-mail do seu amigo ou o domínio que você não deseja filtrar.

7 Clique em **OK**.

Remover amigos

Remova os amigos dessa lista quando desejar filtrá-los.

Para remover amigos:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Amigos**.

5 Selecione o amigo a ser removido e clique em **Remover**.

Atualizando amigos automaticamente

Para garantir que receberá todas as mensagens de seus amigos, você pode importar os respectivos endereços manualmente das listas de endereços ou programar atualizações automáticas.

Importar listas de endereços manualmente

O SpamKiller pode importar suas listas de endereços e atualizar seus amigos.

Para importar listas de endereços manualmente:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Listas de endereços**.

5 Selecione uma lista de endereços a ser importada e, em seguida, clique em **Executar agora**.

6 Clique em **OK**.

Adicionar listas de endereços

Para receber todas as mensagens de seus amigos, certifique-se de que sua lista de endereços esteja incluída na importação.

Para adicionar listas de endereços:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Listas de endereços**.

5 No painel Listas de endereços, clique em **Adicionar**.

6 Clique no tipo de lista de endereços a ser importado na lista **Tipo**.

7 Se aplicável, selecione a origem da lista de endereços na lista **Origem**.

8 Clique em **Diariamente**, **Semanalmente** ou **Mensalmente** na lista **Programação** para determinar quando o SpamKiller verificará se há novos endereços em sua lista de endereços.

9 Clique em **OK**.

Editar listas de endereços

O SpamKiller pode importar suas listas de endereços em intervalos programados e atualizar seus amigos. Você também pode editar as listas de endereços e alterar suas programações de importação.

Para editar as listas de endereços:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Listas de endereços**.

5 Selecione a lista de endereços que você deseja editar e, em seguida, clique em **Editar**.

6 Escolha uma das seguintes opções:

   - Clique no tipo de lista de endereços a ser importado na lista **Tipo**.
   - Se aplicável, selecione a origem da lista de endereços na lista **Origem**.
   - Clique em **Diariamente**, **Semanalmente** ou **Mensalmente** na lista **Programação** para determinar quando o SpamKiller verificará se há novos endereços em sua lista de endereços.

7 Clique em **OK**.

Remover listas de endereços

Remova uma lista de endereços quando não desejar mais importar automaticamente os endereços dela.

Para remover uma lista de endereços da importação automática:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Listas de endereços**.

5 Selecione a lista de endereços a ser removida e, em seguida, clique em **Remover**.

CAPÍTULO 28

Modificando opções de filtragem

As opções de filtragem incluem alteração do nível de filtragem, modificação de filtros especiais, personalização de como as mensagens são manipuladas, especificação dos conjuntos de caracteres a serem filtrados e o relato de spams para a McAfee.

Neste capítulo

Modificando a filtragem de mensagens de e-mail

É possível alterar o rigor com o qual você deseja filtrar as suas mensagens. Se as mensagens de e-mail legítimas estiverem sendo filtradas, você poderá diminuir o nível de filtragem.

Você também pode ativar ou desativar filtros especiais. Por exemplo, mensagens que contêm uma grande proporção de imagens são filtradas, por padrão. Se desejar receber essas mensagens, você poderá desativar esse filtro.

Alterar nível de filtragem de e-mail

É possível alterar o rigor com o qual você deseja filtrar as suas mensagens. Por exemplo, se as mensagens de e-mail legítimas estiverem sendo filtradas, você poderá diminuir o nível de filtragem.

Para alterar o nível de filtragem de e-mail:

1 No Menu avançado, clique em **Configurar**.
2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3 Em **Proteção contra spam**, clique em **Avançado**.
4 No painel Proteção contra spam, clique em **Opções de filtragem**.
5 Em **Opções de filtragem**, mova o botão deslizante para uma das seguintes configurações:
   - **Baixo**: A maioria dos e-mails é aceita.
   - **Médio-Baixo**: Apenas as mensagens de spam óbvias são filtradas.
   - **Médio**: Mais e-mails são aceitos.
   - **Médio-Alto**: Qualquer e-mail semelhante a spam é filtrado.
   - **Alto**: Apenas as mensagens de remetentes em sua lista de Amigos serão aceitas.
6 Clique em **OK**.

Modificar filtros especiais

Você pode ativar ou desativar filtros especiais. Por exemplo, mensagens que contêm uma grande proporção de imagens são filtradas, por padrão. Se desejar receber essas mensagens, você poderá desativar esse filtro.

Para modificar os filtros especiais:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. Selecione **Opções de filtragem**.
5. Em **Filtros especiais**, ative ou desative qualquer uma das seguintes caixas de seleção:
   - **Filtrar mensagens que contêm texto oculto**: O texto oculto é usado para evitar a detecção.
   - **Filtrar mensagens que contêm determinadas proporções de imagens em relação ao texto**: As mensagens que contêm grande proporção de imagens geralmente são spam.
   - **Filtrar mensagens que contêm erros intencionais de formatação HTML**: A formatação inválida é usada para impedir que os filtros filtrem o spam.
   - **Não filtrar mensagens maiores que**: Mensagens maiores do que o valor especificado não serão filtradas. Você pode aumentar ou diminuir o tamanho da mensagem (o intervalo válido é de 0 a 250 KB).
6. Clique em **OK**.

Modificando como as mensagens são processadas

É possível alterar a forma como o spam é identificado e processado. Por exemplo, você pode alterar o nome da marca de phishing ou spam, e indicar se a mensagem será deixada na sua Caixa de entrada ou na pasta do SpamKiller.

Modificar como as mensagens são processadas

É possível alterar a forma como o spam é identificado e processado. Por exemplo, você pode alterar o nome da marca de phishing ou spam, e indicar se a mensagem será deixada na sua Caixa de entrada ou na pasta do SpamKiller.

Para modificar como o SpamKiller processará mensagens de spam:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Processamento**.
5. Escolha uma das seguintes opções:
   - Clique em **Marcar como spam e mover para a pasta do SpamKiller**.

     Essa é a configuração padrão. As mensagens de spam são movidas para a pasta do SpamKiller.
   - Clique em **Marcar como spam e deixar na Caixa de entrada**.

     As mensagens de spam permanecem na sua Caixa de entrada.
   - Digite uma marca personalizada na caixa **Adicione esta marcação personalizada ao assunto de mensagens de spam**.

     A marca que você especificar será adicionada à linha de assunto do e-mail nas mensagens de spam.
   - Digite uma marca personalizada na caixa **Adicione esta marcação personalizada ao assunto de mensagens de phishing**.

     A marca que você especificar será adicionada à linha de assunto do e-mail nas mensagens de phishing.
6. Clique em **OK**.

Filtrando mensagens com conjuntos de caracteres

Os conjuntos de caracteres são usados para representar idiomas, e incluem o alfabeto do idioma, dígitos numéricos e outros símbolos. É possível filtrar mensagens que contenham conjuntos de caracteres específicos. No entanto, não filtre conjuntos de caracteres dos idiomas nos quais você recebe e-mails legítimos.

Por exemplo, se você deseja filtrar mensagens em italiano, mas recebe e-mails legítimos em inglês, não selecione Europeu Ocidental. A seleção de Europeu Ocidental filtrará mensagens em italiano, mas também filtrará mensagens em inglês e em outros idiomas do conjunto de caracteres Europeu Ocidental.

Filtrar mensagens com conjuntos de caracteres

É possível filtrar mensagens que contenham conjuntos de caracteres específicos. No entanto, não filtre conjuntos de caracteres dos idiomas nos quais você recebe e-mails legítimos.

Para filtrar mensagens com conjuntos de caracteres:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Conjuntos de caracteres**.
5. Selecione as caixas de seleção ao lado dos conjuntos de caracteres que você deseja filtrar.
6. Clique em **OK**.

Relatando mensagens de spam

Você pode relatar o spam à McAfee, onde ele será analisado para criar atualizações de filtros.

Relatar mensagens de spam

Você pode relatar o spam à McAfee, onde ele será analisado para criar atualizações de filtros.

Para relatar spam à McAfee:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.

3 Em **Proteção contra spam**, clique em **Avançado**.

4 No painel Proteção contra spam, clique em **Relatando à McAfee**.

5 Marque uma das seguintes caixas de seleção:

- **Ativar geração de relatório ao clicar em Marcar como Spam**: Relatará uma mensagem à McAfee sempre você que marcá-la como spam.
- **Ativar geração de relatório ao clicar em Marcar como não spam**: Relatará uma mensagem à McAfee sempre que você marcá-la como não spam.
- **Enviar mensagem inteira (não apenas cabeçalhos)**: Envia a mensagem inteira, não apenas os cabeçalhos, quando você relata uma mensagem à McAfee.

6 Clique em **OK**.

CAPÍTULO 29

Gerenciando filtros pessoais

Um filtro especifica o que o SpamKiller deve procurar em uma mensagem de e-mail.

O SpamKiller usa vários filtros; no entanto, você pode criar novos filtros ou editar os filtros existentes para fazer um ajuste nas mensagens que são identificadas como spam. Por exemplo, se uma expressão de filtragem contiver "hipoteca", o SpamKiller procurará pelas mensagens que contenham a palavra "hipoteca".

Ao adicionar filtros, examine cuidadosamente a expressão que planeja filtrar. Se for provável que ela apareça em uma mensagem de e-mail normal, não a utilize.

Neste capítulo

Noções básicas sobre como gerenciar filtros pessoais

Esta seção descreve como gerenciar filtros pessoais.

Adicionar filtros pessoais

A criação de filtros é opcional, e eles afetam as mensagens recebidas. Portanto, não crie filtros de palavras comuns que possam aparecer em mensagens que não são spam.

Para adicionar um filtro:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Filtros pessoais**.
5. Clique em **Adicionar**.
6. Na lista **Item**, clique em uma entrada para determinar se o filtro deve procurar por palavras ou expressões no assunto, no corpo, nos cabeçalhos ou no remetente da mensagem.
7. Na lista **Condição**, clique em uma entrada para determinar se o filtro deve procurar por uma mensagem que contenha, ou não, as palavras ou as expressões especificadas.
8. Na caixa **Palavras ou expressões**, digite o que você procura em uma mensagem. Por exemplo, se você especificar "hipoteca", todas as mensagens que contiverem essa palavra serão filtradas.
9. Selecione a caixa de seleção **Este filtro usa expressões regulares (RegEx)** para especificar os padrões de caracteres usados nas condições de filtragem. Para testar um padrão de caracteres, clique em **Testar**.
10. Clique em **OK**.

Editar filtros pessoais

Um filtro especifica o que o SpamKiller deve procurar em uma mensagem de e-mail. O SpamKiller usa vários filtros; no entanto, você pode criar novos filtros ou editar os filtros existentes para fazer um ajuste nas mensagens que são identificadas como spam.

Para editar um filtro:

1 No Menu avançado, clique em **Configurar**.
2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3 Em **Proteção contra spam**, clique em **Avançado**.
4 No painel Proteção contra spam, clique em **Filtros pessoais**.
5 Selecione o filtro que você deseja editar e clique em **Editar**.
6 Na lista **Item**, clique em uma entrada para determinar se o filtro deve procurar por palavras ou expressões no assunto, no corpo, nos cabeçalhos ou no remetente da mensagem.
7 Na lista **Condição**, clique em uma entrada para determinar se o filtro deve procurar por uma mensagem que contenha, ou não, as palavras ou as expressões especificadas.
8 Na caixa **Palavras ou expressões**, digite o que você procura em uma mensagem. Por exemplo, se você especificar "hipoteca", todas as mensagens que contiverem essa palavra serão filtradas.
9 Selecione a caixa de seleção **Este filtro usa expressões regulares (RegEx)** para especificar os padrões de caracteres usados nas condições de filtragem. Para testar um padrão de caracteres, clique em **Testar**.
10 Clique em **OK**.

Remover filtros pessoais

É possível remover filtros que você não deseja mais usar. Quando um filtro é removido, ele é removido definitivamente.

Para remover um filtro:

1 No Menu avançado, clique em **Configurar**.
2 No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3 Em **Proteção contra spam**, clique em **Avançado**.
4 No painel Proteção contra spam, clique em **Filtros pessoais**.
5 Selecione o filtro a ser removido e clique em **Remover**.
6 Clique em **OK**.

Usando expressões regulares

As expressões regulares são caracteres especiais e seqüências que podem ser usados na definição de expressões. Por exemplo:

- A expressão regular **[0-9]*\.[0-9]+**

  corresponde a números flutuantes fornecidos em notação que não é de engenharia. A expressão regular corresponde a: "12.12", ".1212" e "12.0", mas não a "12" e "12."
- A expressão regular **\D*[0-9]+\D***

  corresponde a todas as palavras com números: "SpamKi11er" e "V1AGRA", mas não a "SpamKiller" e "VIAGRA".

Usar expressões regulares

As expressões regulares são caracteres especiais e seqüências que podem ser usados na definição de expressões.

****

Marca o próximo caractere como especial ou literal. Por exemplo, "n" corresponde ao caractere "n". "\n" corresponde a um caractere de nova linha. A seqüência "\\" corresponde a "\" e "\(" corresponde a "(".

^

Corresponde ao início da entrada.

$

Corresponde ao final da entrada.

*

Corresponde ao caractere precedente, zero ou mais vezes. Por exemplo, "zo*" corresponde a "z" ou "zoo".

+

Corresponde ao caractere precedente, uma ou mais vezes. Por exemplo, "zo+" corresponde a "zoo", mas não a "z".

?

Corresponde ao caractere precedente, zero ou uma vez. Por exemplo, "a?va?" corresponde ao "va" de "nevar".

.

Corresponde a qualquer caractere único, exceto o de nova linha.

(padrão)

Corresponde ao padrão e lembra a correspondência. A subseqüência de caracteres correspondente pode ser recuperada da coleção resultante de correspondências, usando o item [0]...[n]. Para corresponder com os caracteres de parêntese ( ), use "\(" ou "\)".

x|y

Corresponde a x ou y. Por exemplo, "m|carro" corresponde a "m" ou "carro". "(m|c)ar" corresponde a "mar" ou "carro".

{n}

O n é um número inteiro não-negativo. Corresponde exatamente a n vezes. Por exemplo, "o{2}" não corresponde ao "o" de "come", mas corresponde aos dois primeiros "o" de "cooooomida".

{n,}

O n é um número inteiro não-negativo. Corresponde a pelo menos n vezes. Por exemplo, "o{2,}" não corresponde ao "o" de "come" e corresponde a todos os "o" de "cooooomida". "o{1,}" equivale a "o+". "o{0,}" equivale a "o*".

{n,m}

m e n são números inteiros não-negativos. Correspondem a no mínimo n e no máximo m vezes. Por exemplo, "o{1,3}" corresponde aos três primeiros "o" de "cooooomida". "o{0,1}" equivale a "o?".

[xyz]

Um conjunto de caracteres. Corresponde a qualquer um dos caracteres entre colchetes. Por exemplo, "[abc]" corresponde ao "a" de "plano".

[^xyz]

Um conjunto negativo de caracteres. Corresponde a qualquer caractere não especificado entre colchetes. Por exemplo, "[^abc]" corresponde ao "p" de "plano".

[a-z]

Um intervalo de caracteres. Corresponde a qualquer caractere do intervalo especificado. Por exemplo, "[a-z]" corresponde a qualquer caractere alfabético em maiúscula ou minúscula no intervalo de "a" a "z" e de "A" a "Z".

[A-Z]

Um intervalo de caracteres. Corresponde a qualquer caractere do intervalo especificado. Por exemplo, "[A-Z]" corresponde a qualquer caractere alfabético em maiúsculas ou minúsculas no intervalo de "A" a "Z" e de "a" a "z".

[^m-z]

Os caracteres de um intervalo negativo. Corresponde a qualquer caractere que não esteja no intervalo especificado. Por exemplo, "[^m-z]" corresponde a qualquer caractere que não seja de "m" a "z".

\b

Corresponde a um limite de palavra, ou seja, a posição entre uma palavra e um espaço. Por exemplo, "er\b" corresponde ao "er" de "comer", mas não ao "er" de "verbo".

\B

Corresponde à ausência de um limite de palavra. "an*t\B" corresponde ao "ant" de "nunca antes".

\d

Corresponde a um caractere numérico. Equivale a [0-9].

\D

Corresponde a um caractere não-numérico. Equivale a [^0-9].

\f

Corresponde ao caractere de avanço de página.

\n

Corresponde ao caractere de nova linha.

\r

Corresponde ao caractere de retorno de carro.

\s

Corresponde a qualquer espaço em branco, incluindo espaço, tabulação, avanço de página, etc. Equivale a "[\f\n\r\t\v]".

\S

Corresponde a qualquer caractere de espaço que não esteja em branco. Equivale a "[^ \f\n\r\t\v]".

\t

Corresponde a um caractere de tabulação.

\v

Corresponde a um caractere de barra vertical.

\w

Corresponde a qualquer caractere alfanumérico ou "_”. Equivale a "[A-Za-z0-9_]".

\W

Corresponde a qualquer caractere que não seja alfanumérico ou "_”. Equivale a "[^A-Za-z0-9_]".

\num

Corresponde a num, onde num é um número inteiro positivo. Uma referência às correspondências lembradas. Por exemplo, "(.)\1" corresponde a dois caracteres idênticos consecutivos. \n corresponde a n, onde n é um valor octal de escape. Os valores de escape octais devem conter 1, 2 ou 3 dígitos. Por exemplo, "\11" e "\011" coincidem ambos com um caractere de tabulação. "\0011" é o equivalente de "\001" & "1". Os valores de escape octais não devem exceder 256. Caso excedam, somente os dois primeiros dígitos formarão a expressão. Permite o uso de códigos ASCII em expressões regulares.

\xn

Corresponde a n, onde n é um valor de escape hexadecimal. Os valores de escape hexadecimais devem conter exatamente dois dígitos. Por exemplo, "\x41" corresponde a "A". "\x041" é equivalente a "\x04" & "1". Permite o uso de códigos ASCII em expressões regulares.

CAPÍTULO 30

Mantendo o SpamKiller

A manutenção do SpamKiller inclui o gerenciamento da proteção contra spam e a utilização das barras de ferramentas.

Ao gerenciar a proteção contra spam, você pode desativar ou ativar a filtragem.

Ao usar as barras de ferramentas, você pode desativar ou ativar as barras de ferramentas de e-mail fornecidas pelo SpamKiller e marcar as mensagens como spam ou não spam a partir da barra de ferramentas.

Neste capítulo

Gerenciando a proteção contra spam

Você pode desativar ou ativar a filtragem de mensagens de e-mail.

Desative a proteção contra spam para evitar que mensagens de e-mail sejam filtradas ou ative a proteção contra spam para filtrar mensagens de e-mail.

Desativar a proteção contra spam

Você pode desativar a proteção contra spam e impedir mensagens de e-mail sejam filtradas.

Para desativar a filtragem:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Desligado**.

Ativar a proteção contra spam

Você pode ativar a proteção contra spam e filtrar mensagens de e-mail.

Para ativar a filtragem:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Ligado**.

Usando as barras ferramentas

Você pode desativar ou ativar as barras de ferramentas de e-mail dos clientes de e-mail suportados.

Se estiver usando os programas de e-mail Outlook, Outlook Express, Windows Mail, Eudora ou Thunderbird, você também poderá marcar as mensagens como spam ou não spam a partir da barra de ferramentas do SpamKiller.

Desativar uma barra de ferramentas

Você pode desativar as barras de ferramentas dos clientes de e-mail suportados.

Para desativar uma barra de ferramentas:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Barras de ferramentas de e-mail** e desmarque a caixa de seleção ao lado da barra de ferramentas que você deseja desativar.
5. Clique em **OK**.

Ativar uma barra de ferramentas

Se você desativar alguma barra de ferramentas, poderá ativá-la novamente.

Para ativar uma barra de ferramentas:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **E-mail e mensagens instantâneas**.
3. Em **Proteção contra spam**, clique em **Avançado**.
4. No painel Proteção contra spam, clique em **Barras de ferramentas de e-mail** e marque a caixa de seleção ao lado da barra de ferramentas que você deseja ativar.
5. Clique em **OK**.

Marcar mensagens como spam ou não spam a partir da barra de ferramentas do SpamKiller

Se estiver usando os programas de e-mail Outlook, Outlook Express, Windows Mail, Eudora ou Thunderbird, você poderá marcar as mensagens como spam ou não spam a partir da barra de ferramentas do SpamKiller.

Ao marcar uma mensagem como spam, a mensagem é identificada com [SPAM] ou uma marcação de sua escolha e é deixada em sua Caixa de entrada, pasta do SpamKiller (Outlook, Outlook Express, Windows Mail, Thunderbird) ou pasta Lixo eletrônico (Eudora).

Quando você marca uma mensagem como não spam, a marcação é removida, e a mensagem é movida para a sua Caixa de entrada.

Para marcar as mensagens como spam ou não spam no Outlook:

1. No seu programa de e-mail, selecione uma mensagem.
2. Na barra de ferramentas do **SpamKiller**, clique em **Marcar como spam** ou **Marcar como não spam**.

Para marcar as mensagens como spam ou não spam no Outlook Express, no Windows Mail, no Eudora ou no Thunderbird:

1. No seu programa de e-mail, selecione uma mensagem.
2. No menu **SpamKiller**, clique em **Marcar como spam** ou **Marcar como não spam**.

CAPÍTULO 31

Configurando a proteção contra phishing

O e-mail não solicitado é classificado como spam (e-mails que solicitam que você adquira algo) ou phishing (e-mails que solicitam que você forneça informações pessoais para um site potencialmente ou sabidamente fraudulento).

O filtro Phishing ajuda a protegê-lo contra sites fraudulentos. Ao navegar em um site fraudulento (conhecido ou potencial), você será redirecionado para a página do filtro Phishing.

Você pode desativar ou ativar a proteção contra phishing ou modificar as opções de filtragem.

Neste capítulo

Desativando ou ativando a proteção contra phishing

Você pode desativar ou ativar a proteção contra phishing. Por exemplo, desative a proteção contra phishing quando você estiver tentando acessar um site de sua confiança que esteja sendo bloqueado.

Desativar proteção contra phishing

Desative a proteção contra phishing quando você estiver tentando acessar um site de sua confiança que esteja sendo bloqueado.

Para desativar a proteção contra phishing:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Internet e Rede**.
3. Em **Phishing**, clique em **Desligado**.

Ativar proteção contra phishing

Ative a proteção contra phishing para assegurar-se de que esteja protegido contra sites de phishing.

Para ativar a proteção contra phishing:

1. No Menu avançado, clique em **Configurar**.
2. No painel Configurar, clique em **Internet e Rede**.
3. Em **Phishing**, clique em **Ligado**.

Modificando a filtragem de phishing

Existem duas maneiras através das quais a McAfee determina se um site da Web é um site de phishing ou não: comparando o site que você está visualizando com uma lista de sites fraudulentos conhecidos, ou tentando determinar se o site que você está visualizando é fraudulento.

Modificar a filtragem de phishing

Existem duas maneiras através das quais a McAfee determina se um site da Web é um site de phishing ou não. Para receber proteção total, deixe ambas as opções selecionadas.

Para alterar as opções de phishing:

1 No Menu avançado, clique em **Configurar**.

2 No painel Configurar, clique em **Internet e Rede**.

3 Em **Phishing**, clique em **Avançado**.

4 Ative ou desative qualquer uma das seguintes caixas de seleção:

   - **Ativar pesquisas de lista negra e lista branca para detectar sites da Web fraudulentos**: Compara o site da Web que você está exibindo com uma lista de sites fraudulentos conhecidos.
   - **Ativar heurística para detectar sites da Web fraudulentos**: Tenta determinar se o site da Web que você está exibindo é fraudulento.

5 Clique em **OK**.

CAPÍTULO 32

Ajuda adicional

Este capítulo descreve as perguntas freqüentes.

Neste capítulo

Perguntas freqüentes

Esta seção fornece as respostas para as perguntas mais freqüentes.

O que são contas POP3, MSN/Hotmail e MAPI?

O SpamKiller foi criado para trabalhar com estes tipos de contas de e-mail: POP3, Web Mail POP3, MSN/Hotmail e MAPI. Há algumas diferenças entre elas, o que afeta a forma como o SpamKiller executa a filtragem.

POP3

É o tipo de conta mais comum e é o padrão para e-mails de Internet. Quando você possui uma conta POP3, o SpamKiller se conecta diretamente ao servidor e filtra as mensagens antes que sejam recuperadas pelo programa de e-mail.

Web Mail POP3

As contas de Web Mail POP3 são baseadas na Web. A filtragem das contas de Web Mail POP3 é semelhante à filtragem das contas POP3.

MSN/Hotmail

As contas MSN/Hotmail são baseadas na Web. A filtragem de contas MSN/Hotmail é semelhante à filtragem de contas POP3.

MAPI

O MAPI é um sistema criado pela Microsoft para suporte a vários tipos de mensagens, inclusive e-mails da Internet, fax e mensagens do Exchange Server. Por isso, normalmente o MAPI é usado em ambientes corporativos quando a empresa possui o Microsoft ® Exchange Server. Porém, muitas pessoas usam o Microsoft Outlook como e-mail pessoal da Internet. O SpamKiller pode acessar contas MAPI, mas observe o seguinte:

- Em geral, a filtragem só é executada após a recuperação das mensagens pelo programa de e-mail.
- O SpamKiller filtra somente a caixa de entrada padrão e as mensagens de e-mail da Internet.

O que é filtro phishing?

O e-mail não solicitado é classificado como spam (e-mails que solicitam que você adquira algo) ou phishing (e-mails que solicitam que você forneça informações pessoais para um site potencialmente ou sabidamente fraudulento).

O filtro Phishing ajuda a protegê-lo contra sites que estejam na lista negra (phishing confirmado ou sites fraudulentos associados) ou na lista cinza (com algum conteúdo perigoso ou links para sites da lista negra).

Ao navegar em um site fraudulento conhecido ou potencial, você será redirecionado para a página do filtro Phishing.

Por que a McAfee usa cookies?

O site da McAfee na Web utiliza marcas de software chamadas cookies para identificar clientes que visitam o site mais de uma vez. Os cookies são blocos de texto inseridos em um arquivo na unidade de disco rígido do seu computador. Eles são usados para identificá-lo quando você volta a acessar o site.

A McAfee utiliza cookies para:

- Gerenciar os seus direitos e permissões de assinatura
- Identificá-lo como usuário antigo para não ser necessário novo registro a cada visita
- Entender as suas preferências de compras e personalizar serviços de acordo com suas necessidades
- Apresentar informações, produtos e ofertas especiais que possam interessá-lo

A McAfee também solicita que você forneça seu nome, a fim de personalizar sua experiência no site.

A McAfee não pode fornecer serviços de assinatura a usuários cujos navegadores estejam configurados para rejeitar cookies. Ela não vende, não aluga, nem compartilha com terceiros as informações coletadas.

A McAfee permite que anunciantes coloquem cookies nos navegadores dos visitantes. Ela não tem acesso às informações contidas nos cookies dos anunciantes.

CAPÍTULO 33

McAfee Privacy Service

O Privacy Service oferece proteção avançada para você, sua família, seus dados pessoais e seu computador. Ele o ajuda a se proteger contra roubos de identidade on-line, bloquear a transmissão de informações de identificação pessoal e filtrar conteúdos on-line potencialmente ofensivos (incluindo imagens, anúncios, pop-ups e Web bugs). Também oferece controles avançados pelos pais, permitindo que os adultos monitorem, controlem e registrem os hábitos de navegação de crianças, além de proteger a área de armazenamento com senhas.

Antes de começar a usar o Privacy Service, você pode se familiarizar com alguns dos recursos mais populares. A Ajuda do Privacy Service fornece detalhes sobre como configurar e usar esses recursos.

Neste capítulo

Recursos

O Privacy Service oferece os seguintes recursos:

- Proteção de navegação na Web
- Proteção de informações pessoais
- Parental Controls
- Armazenamento de senha

Proteção de navegação na Web

A proteção da navegação da Web permite que você bloqueie anúncios, pop-ups e Web bugs em seu computador. O bloqueio de anúncios e janelas pop-up impede a exibição da maioria dos anúncios e janelas pop-up no navegador. O bloqueio de Web bugs impede que os sites da Web rastreiem atividades on-line e enviem informações a fontes não autorizadas. O bloqueio combinado de anúncios, pop-ups e Web bugs aumenta a segurança e impede que conteúdos não solicitados atrapalhem sua navegação na Web.

Proteção de informações pessoais

A proteção de informações pessoais permite que você bloqueie a transmissão de informações importantes ou confidenciais (por exemplo, números de cartões de crédito, números de contas bancárias, endereços, etc.) pela Internet.

Controles pelos pais

Os controles pelos pais permitem que você configure as classificações de conteúdo, que restringem os sites e o conteúdo que um usuário pode exibir, bem como os limites de horário da Internet, que especificam o período e a duração em que um usuário pode acessar a Internet. Eles também permitem que você restrinja universalmente o acesso a sites da Web específicos, além de conceder e bloquear o acesso com base em faixa etária e palavras-chave associadas.

Armazenamento de senha

O Cofre de senhas é uma área segura de armazenamento para suas senhas pessoais. Ele permite que você guarde suas senhas, garantindo que nenhum outro usuário (nem mesmo um Administrador McAfee ou administrador do sistema) poderá acessá-las.

CAPÍTULO 34

Configurando os controles pelos pais

Depois de adicionar um usuário, configure os controles pelos pais desse usuário. Os controles pelos pais são configurações que definem os grupos de classificação de conteúdo, nível de bloqueio de cookies e os limites de horário na Internet. Os grupos de classificação de conteúdo determinam o tipo de conteúdo da Internet e os sites que podem ser acessados pelo usuário, com base em sua faixa etária. O nível de bloqueio de cookies determina se os sites podem ou não ler os cookies que definiram no computador, quando o usuário estiver conectado. Os limites de horário na Internet definem os dias e as horas em que o usuário pode acessar a Internet.

Você também pode configurar alguns controles de restrição para menores, que se aplicam a qualquer usuário que não seja adulto. Por exemplo, você pode bloquear ou permitir determinados sites, ou impedir que imagens potencialmente inadequadas sejam exibidas quando usuários que não sejam adultos estiverem navegando na Internet. Você também pode definir as configurações de bloqueio de cookies global para todos os usuários. Contudo, se um nível de bloqueio de cookies de usuário individual for diferente das configurações de bloqueio de cookies globais, as configurações globais terão prioridade.

Observação: É necessário ser um Administrador para configurar os controles pelos pais.

Neste capítulo

Configurando um grupo de classificação de conteúdo do usuário

Um usuário pode pertencer a um dos seguintes grupos de classificação de conteúdo:

- Criança pequena
- Criança
- Pré-adolescente
- Adolescente
- Adulto

O conteúdo é classificado (ou seja, disponibilizado ou bloqueado) com base no grupo ao qual o usuário pertence. Por exemplo, determinados sites são bloqueados para os usuários que pertencem ao grupo de crianças pequenas, mas podem ser acessados por usuários que pertencem ao grupo de adolescentes. Os usuários que pertencem ao grupo de adultos podem acessar todos os conteúdos. Por padrão, um novo usuário é automaticamente adicionado ao grupo de crianças pequenas, com todas as restrições aplicadas ao conteúdo disponível para esse grupo.

Como Administrador, você pode definir o grupo de classificação de conteúdo de um usuário e, em seguida, bloquear ou permitir sites com base nesses grupos. Se desejar classificar o conteúdo para um usuário mais estritamente, você também pode evitar que o usuário navegue em sites que não estejam incluídos na lista global **Sites da Web permitidos**. Para obter mais informações, consulte Bloquear sites com base em palavras-chave (página 241) e Permitindo sites (página 242).

Configurar o grupo de classificação de conteúdo do usuário

Um grupo de classificação de conteúdo para usuário é uma faixa etária que determina o tipo de conteúdo da Internet e de sites disponível para o usuário.

Para configurar o grupo de classificação de conteúdo para um usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Classificação de conteúdo**, clique na faixa etária que deseja atribuir ao usuário.
   Em seguida, você poderá classificar conteúdos de acordo com cada faixa etária, permitindo o bloqueio da exibição de conteúdos inadequados a um determinado nível de maturidade ou idade.
7. Para restringir o acesso do usuário a sites que não estão incluídos na lista global **Sites da Web permitidos**, marque a caixa de seleção **Restringir esse usuário aos sites da lista "Sites da Web permitidos"**.
8. Clique em **OK**.

Configurando o nível de bloqueio de cookies de um usuário

Alguns sites criam pequenos arquivos, chamados *cookies*, em seu computador, para monitorar suas preferências pessoais e seus hábitos de navegação. Como Administrador, você pode atribuir um dos seguintes níveis de bloqueio de cookies a um usuário:

- Aceitar todos os cookies
- Rejeitar todos os cookies
- Perguntar ao usuário se ele aceitará cookies

A definição de aceitar todos os cookies permite que sites da Web leiam os cookies que colocam em seu computador quando o usuário correspondente se conecta. A configuração de rejeitar todos os cookies impede que sites da Web leiam os cookies. A definição de perguntar ao usuário se ele aceitará os cookies solicita que o usuário confirme cada vez que um site da Web tentar colocar um cookie em seu computador. O usuário poderá decidir se aceitará ou rejeitará cookies de acordo com cada caso. Depois que o usuário decide aceitar ou rejeitar cookies para um determinado site, ele não será mais solicitado para esse site.

Observação: Para que alguns sites da Web funcionem adequadamente, é necessário ativar os cookies.

Configurar o nível de bloqueio de cookies de um usuário

Alguns sites criam pequenos arquivos, chamados *cookies*, em seu computador, para monitorar suas preferências pessoais e seus hábitos de navegação. Você pode especificar como deseja que os cookies sejam tratados para cada usuário em seu computador.

Para configurar o nível de bloqueio de cookies de um usuário:

1. Em **Tarefas comuns**, clique em **Início**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, em **Usuários**, clique em **Avançado**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Bloqueio de cookies**, escolha uma das seguintes opções:
   - **Aceitar todos os cookies:** Todos os sites que este usuário visitar podem ler os cookies colocados no computador.

- **Rejeitar todos os cookies:** Nenhum dos sites que este usuário visitar pode ler os cookies colocados no computador.
- **Perguntar ao usuário para aceitar cookies:** Quando este usuário tentar visitar um site da Web, aparecerá uma mensagem perguntando se o usuário permite ou rejeita cookies.

7 Clique em **OK**.

Adicionar um site à lista de cookies aceitos do usuário

Se configurar um nível de bloqueio de cookies do usuário para solicitar permissão para que sites definam cookies, mas desejar permitir sempre que determinados sites definam cookies sem essa solicitação, você pode adicionar esses sites à lista de cookies aceitos do usuário.

Para adicionar um site à lista de cookies aceitos do usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Bloqueio de cookies**, clique em **Exibir lista**.
7. Em **Aceitar cookies de sites da Web**, digite o endereço de um site na caixa **http://** e, em seguida, clique em **Adicionar**.
8. Clique em **Concluído**.

Modificar um site na lista de cookies aceitos do usuário

Se o endereço de um site mudar ou for digitado incorretamente na lista de cookies aceitos do usuário, você poderá alterá-lo.

Para modificar um site na lista de cookies aceitos do usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Bloqueio de cookies**, clique em **Exibir lista**.
7. Em **Aceitar cookies de sites da Web**, clique em uma entrada da lista **Sites da Web**, modifique o endereço do site na caixa **http://** e clique em **Atualizar**.
8. Clique em **Concluído**.

Remover um site da lista de cookies aceitos do usuário

Se adicionar um site por engano à lista de cookies aceitos do usuário, você poderá removê-lo.

Para remover um site da lista de cookies aceitos do usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Bloqueio de cookies**, clique em **Exibir lista**.
7. Em **Aceitar cookies de sites da Web**, clique em uma entrada da lista **Sites da Web** e, em seguida, clique em **Remover**.
8. Na caixa de diálogo Confirmação de remoção, clique em **Sim**.
9. Clique em **Concluído**.

Adicionar um site à lista de cookies rejeitados de um usuário

Se configurar um nível de bloqueio de cookies do usuário para solicitar permissão para que sites definam cookies, mas quiser evitar sempre que determinados sites configurem cookies sem essa solicitação, você pode adicionar esses sites à lista de cookies aceitos do usuário.

Para adicionar um site à lista de cookies rejeitados do usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Bloqueio de cookies**, clique em **Exibir lista**.
7. Clique em **Rejeitar cookies de sites da Web**.
8. Em **Rejeitar cookies de sites da Web**, digite o endereço de um site na caixa **http://** e, em seguida, clique em **Adicionar**.
9. Clique em **Concluído**.

Modificar um site na lista de cookies rejeitados do usuário

Se o endereço de um site mudar ou se tiver sido digitado incorretamente na lista de cookies rejeitados do usuário, você poderá alterá-lo.

Para modificar um site na lista de cookies rejeitados do usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Bloqueio de cookies**, clique em **Exibir lista**.
7. Clique em **Rejeitar cookies de sites da Web**.
8. Em **Rejeitar cookies de sites da Web**, clique em uma entrada da lista **Sites da Web**, modifique o endereço do site na caixa **http://** e clique em **Atualizar**.
9. Clique em **Concluído**.

Remover um site da lista de cookies rejeitados do usuário

Se adicionar um site por engano à lista de cookies rejeitados do usuário, você poderá removê-lo.

Para remover um site da lista de cookies rejeitados do usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Bloqueio de cookies**, clique em **Exibir lista**.
7. Clique em **Rejeitar cookies de sites da Web**.
8. Em **Rejeitar cookies de sites da Web**, clique em uma entrada da lista **Sites** e, em seguida, clique em **Remover**.
9. Na caixa de diálogo Confirmação de remoção, clique em **Sim**.
10. Clique em **Concluído**.

Configurando os limites de horário de Internet de um usuário

Como administrador, você pode usar a grade Limites de horário para uso da Internet para especificar se e quando um usuário pode acessar a Internet. Você pode conceder uso irrestrito da Internet, uso limitado da Internet ou proibir completamente o uso da Internet.

A grade de limites de horário para uso da Internet permite especificar limites de horário em intervalos de trinta minutos. As partes verdes da grade representam os dias e horários em que o usuário pode acessar a Internet. As partes vermelhas da grade representam os dias e horários durante os quais o acesso é negado. Se um usuário tentar acessar a Internet durante um período proibido, a McAfee notificará o usuário de que isso não é permitido.

Se você proibir um usuário de acessar a Internet completamente, esse usuário poderá efetuar logon e usar o computador, mas não a Internet.

Definir os limites de horário na Internet de um usuário

Você usa a grade de limites de horário na Internet para especificar quando um determinado usuário poderá acessar a Internet. As áreas verdes da grade representam os dias e os horários em que o usuário pode acessar a Internet. As áreas vermelhas da grade representam os dias e os horários em que o acesso é negado.

Para definir os limites de horário na Internet para o usuário:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. Em **Informações do SecurityCenter**, clique em **Configurar**.
3. No painel Configuração do SecurityCenter, clique em **Avançado** em **Usuários**.
4. No painel Usuários, clique em **Controles pelos pais**.
5. Selecione um nome de usuário na lista.
6. Em **Limites de horário na Internet**, pressione e arraste para especificar os dias e os horários em que esse usuário pode acessar a Internet.
7. Clique em **OK**.

Bloqueando sites da Web

Se você for um Administrador e desejar impedir que todos os usuários não-adultos acessem um determinado site da Web, você poderá bloquear o site. Quando um usuário tentar acessar um site bloqueado, aparecerá uma imagem indicando que o site não pode ser acessado porque está bloqueado pela McAfee.

Os usuários (incluindo os administradores) que pertencem à faixa etária adulta podem acessar todos os sites da Web, mesmo que estejam na lista **Sites bloqueados**. Para testar os sites da Web bloqueados, você deve efetuar logon como um usuário não-adulto.

Como Administrador, você também pode bloquear sites da Web com base em palavras-chave que os sites contenham. A McAfee mantém uma lista padrão de palavras-chave e regras correspondentes, que determina se um usuário de uma determinada faixa etária pode ou não visitar um site que contenha essa palavra-chave. Quando a varredura de palavra-chave está ativada, a lista padrão de palavras-chave é usada para classificar o conteúdo para os usuários. No entanto, você pode adicionar suas próprias palavras permitidas à lista padrão e associá-las a determinadas faixas etárias. Regras de palavras-chave que você adiciona substituem uma possível regra existente que possa estar associada a palavra-chave igual na lista padrão. É possível usar palavras-chave existentes ou especificar novas palavras-chave para associar a determinadas faixas etárias.

Bloquear um site.

Você pode bloquear um site se desejar evitar que todos os usuários que não sejam adultos acessem o site. Se um usuário tentar acessar o site, será exibida uma mensagem indicando que o site foi bloqueado pela McAfee.

Para bloquear um site:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3. Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4. No painel Configuração dos controles pelos pais, certifique-se de que os Controles pelos pais estão ativados e, em seguida, clique em **Avançado**.
5. No painel Sites da Web bloqueados, digite um endereço de site na caixa **http://** e, em seguida, clique em **Adicionar**.
6. Clique em **OK**.

Modificar um site bloqueado

Se o endereço de um site mudar ou for digitado incorretamente na lista Sites da Web bloqueados, você poderá alterá-lo.

Para modificar um site bloqueado:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3. Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4. No painel Configuração dos controles pelos pais, clique em **Avançado**.
5. No painel Sites bloqueados, clique em uma entrada da lista **Sites da Web bloqueados**, modifique o endereço do site na caixa **http://** e clique em **Atualizar**.
6. Clique em **OK**.

Remover um site bloqueado

Se não desejar mais bloquear um site, você deverá removê-lo da lista **Sites da Web bloqueados**.

Para remover um site bloqueado:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3. Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4. No painel Configuração dos controles pelos pais, clique em **Avançado**.
5. No painel Sites da Web bloqueados, clique em uma entrada da lista **Sites da Web bloqueados** e, em seguida, clique em **Remover**.
6. Na caixa de diálogo Confirmação de remoção, clique em **Sim**.
7. Clique em **OK**.

Desativar a varredura de palavra-chave

Por padrão, a varredura de palavra-chave está ativada, o que significa que a lista padrão de palavras-chave da McAfee é usada para classificar o conteúdo para os usuários. Embora a McAfee não recomende esse procedimento, você pode desativar a varredura de palavra-chave a qualquer momento.

Para desativar varredura de palavra-chave:

1 Em **Tarefas comuns**, clique em **Início**.

2 No painel Início do SecurityCenter, clique em **Controles pelos pais**.

3 Na seção de informações dos Controles pelos pais, clique em **Configurar**.

4 No painel Configuração dos controles pelos pais, clique em **Avançado**.

5 No painel Controles de restrição para menores, clique em **Varredura de palavra-chave**.

6 No painel Varredura de palavra-chave, clique em **Desligado**.

7 Clique em **OK**.

Bloquear sites com base em palavras-chave

Se quiser bloquear sites com determinados conteúdos e não souber seus endereços exatos, utilize suas palavras-chave para bloqueá-los. Basta inserir uma palavra-chave e depois determinar quais faixas etárias podem ou não podem visualizar os sites que contêm essa palavra-chave.

Para bloquear sites com base em palavras-chave:

1 Em **Tarefas comuns**, clique em **Iniciar**.

2 No painel Início do SecurityCenter, clique em **Controles pelos pais**.

3 Na seção de informações dos Controles pelos pais, clique em **Configurar**.

4 No painel Configuração dos controles pelos pais, clique em **Avançado**.

5 No painel Controles de restrição para menores, clique em **Varredura de palavra-chave** e certifique-se de que essa opção esteja ativada.

6 No painel Controles de restrição para menores, clique em **Palavras-chave**.

7 Digite uma palavra-chave na caixa **Procurar**.
Os sites que contêm essa palavra serão bloqueados.

8 Mova o botão deslizante **Idade mínima** para especificar a faixa etária mínima.
Os usuários dessa faixa etária e acima dela poderão exibir os sites que contêm a palavra-chave.

9 Clique em **OK**.

Permissão de sites

Se você for um Administrador, poderá permitir que todos os usuários acessem um determinado site, substituindo quaisquer configurações padrão e sites bloqueados.

Para obter mais informações sobre sites bloqueados, consulte Bloqueando sites da Web (página 238).

Permitir um site

Se desejar garantir que um site não seja bloqueado para nenhum usuário, adicione o endereço do site à lista **Sites permitidos**. Quando você adiciona um site à lista **Sites permitidos**, substitui quaisquer configurações padrão e sites adicionados anteriormente à lista **Sites bloqueados**.

Para permitir um site da Web:

1. Em **Tarefas comuns**, clique em **Início**.
2. No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3. Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4. No painel Configuração dos controles pelos pais, clique em **Avançado**.
5. No painel Controles de restrição para menores, clique em **Sites permitidos**.
6. No painel Sites permitidos, digite o endereço de um site da Web na caixa **http://** e clique em **Adicionar**.
7. Clique em **OK**.

Dica: Você pode impedir que um usuário navegue em quaisquer sites que não estejam incluídos na lista **Sites permitidos**. Para obter mais informações, consulte Configurando o grupo de classificação de conteúdo de um usuário (página 230).

Modificar um site da Web permitido

Se o endereço de um site mudar ou for digitado incorretamente na lista **Sites da Web permitidos**, você poderá alterá-lo.

Para modificar um site permitido:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3. Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4. No painel Configuração dos controles pelos pais, clique em **Avançado**.
5. No painel Controles de restrição para menores, clique em **Sites permitidos**.
6. No painel Sites da Web permitidos, clique em uma entrada da lista **Sites da Web permitidos**, modifique o endereço do site na caixa **http://** e clique em **Atualizar**.
7. Clique em **OK**.

Remover um site permitido

Você pode remover um site permitido quando desejar. Dependendo das configurações que você definir, quando um site for removido da lista **Sites da Web permitidos**, talvez os usuários do McAfee não possam mais acessá-lo.

Para remover um site permitido:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3. Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4. No painel Configuração dos controles pelos pais, clique em **Avançado**.
5. No painel Controles de restrição para menores, clique em **Sites permitidos**.
6. No painel Sites da Web permitidos, clique em uma entrada da lista **Sites da Web permitidos** e, em seguida, clique em **Remover**.
7. Na caixa de diálogo Confirmação de remoção, clique em **Sim**.
8. Clique em **OK**.

Permitindo que sites definam cookies

Se impedir que todos os sites leiam os cookies definidos no computador ou configurar determinados usuários para receberem uma mensagem de solicitação antes que o cookie seja aceito e, em seguida, achar que alguns sites não estão funcionando adequadamente, você poderá permitir que eles leiam seus cookies.

Para obter mais informações sobre cookies e nível de bloqueio de cookies, consulte Configurando o nível de bloqueio de cookies de um usuário (página 232).

Permitir que um site defina cookies

Se impedir que todos os sites leiam os cookies definidos no computador ou configurar determinados usuários para receberem uma mensagem de solicitação antes que o cookie seja aceito e, em seguida, achar que alguns sites não estão funcionando adequadamente, você poderá permitir que eles leiam seus cookies.

Para permitir que um site defina cookies:

1 Em **Tarefas comuns**, clique em **Iniciar**.

2 No painel Início do SecurityCenter, clique em **Controles pelos pais**.

3 Na seção de informações dos Controles pelos pais, clique em **Configurar**.

4 No painel Configuração dos controles pelos pais, clique em **Avançado**.

5 No painel Controles de restrição para menores, clique em **Cookies**.

6 No painel Cookies, digite um endereço de site na caixa **http://** e, em seguida, clique em **Adicionar**.

7 Clique em **OK**.

Modificar a lista Aceitar cookies

Se o endereço de um site mudar ou for inserido incorretamente, quando adicioná-lo à lista **Aceitar cookies**, você poderá alterá-lo.

Para modificar a lista de Cookies:

1 Em **Tarefas comuns**, clique em **Iniciar**.
2 No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3 Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4 No painel Configuração dos controles pelos pais, clique em **Avançado**.
5 No painel Controles de restrição para menores, clique em **Cookies**.
6 No painel Cookies permitidos, clique em uma entrada da lista **Aceitar cookies**, modifique o endereço na caixa **http://** e clique em **Atualizar**.
7 Clique em **OK**.

Evitar que um site defina cookies

Se quiser evitar que um site específico leia os cookies que definiu no computador, remova-o da lista **Aceitar cookies**.

Para evitar que um site defina cookies:

1 Em **Tarefas comuns**, clique em **Iniciar**.
2 No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3 Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4 No painel Configuração dos controles pelos pais, clique em **Avançado**.
5 No painel Controles de restrição para menores, clique em **Cookies**.
6 No painel Cookies, clique em uma entrada da lista **Aceitar cookies** e, em seguida, clique em **Remover**.
7 Na caixa de diálogo Confirmação de remoção, clique em **Sim**.
8 Clique em **OK**.

Bloqueando imagens da Web potencialmente inadequadas

Proteja sua família, bloqueando a exibição de imagens potencialmente inadequadas durante a navegação na Internet. As imagens podem ser bloqueadas para todos os usuários ou para todos exceto os membros da faixa etária adulta. Para obter mais informações sobre faixas etárias, consulte Configurando o grupo de classificação de conteúdo de um usuário (página 230).

Por padrão, a análise de imagens é ativada para todos os usuários, exceto os da faixa etária adulta, mas como Administrador você pode desativá-la a qualquer momento.

Bloquear imagens potencialmente inadequadas

Por padrão, a McAfee permite a análise de imagens, protegendo sua família através do bloqueio de imagens potencialmente inadequadas, durante a utilização da Internet. Se a McAfee detectar uma imagem potencialmente inadequada, ele a substituirá por uma imagem personalizada, indicando que a original foi bloqueada. É necessário ser um Administrador para desativar a análise de imagens.

Para bloquear imagens potencialmente inadequadas:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Controles pelos pais**.
3. Na seção de informações dos Controles pelos pais, clique em **Configurar**.
4. No painel Configuração dos controles pelos pais, clique em **Avançado**.
5. No painel Controles de restrição para menores, clique em **Análise de imagens**.
6. No painel Análise de imagens, execute um dos procedimentos a seguir:
   - Clique em **Todos os usuários** para bloquear imagens potencialmente inadequadas para todos os usuários.
   - Clique em **Adolescentes e crianças** para bloquear imagens potencialmente inadequadas para todos os usuários, exceto membros da faixa etária adulta.
7. Clique em **OK**.

CAPÍTULO 35

Protegendo informações na Internet

Use o Privacy Service para proteger sua família e informações pessoais ao navegar na Internet. Por exemplo, se for um Administrador, você poderá configurar a McAfee para bloquear anúncios, pop-ups e Web bugs quando os usuários estiverem na Internet. Também é possível impedir que suas informações pessoais (como nome, endereço, números de cartão de crédito e números de contas bancárias) sejam transmitidas pela Internet, adicionando-as à área de informações bloqueadas.

Neste capítulo

Bloqueando anúncios, pop-ups e Web bugs

Se você for um Administrador, poderá configurar a McAfee para bloquear anúncios, pop-ups e Web bugs quando os usuários estiverem utilizando a Internet. O bloqueio de anúncios e janelas pop-ups impede a exibição da maioria dos anúncios e janelas pop-ups no navegador da Web. Isso pode ajudá-lo a melhorar a velocidade e a eficiência de sua navegação na Internet. O bloqueio de Web bugs impede que os sites da Web rastreiem atividades on-line e enviem informações a fontes não autorizadas. Os Web bugs (também chamados de beacons da Web, marcas de pixel, GIFs de limpeza ou GIFs invisíveis) são arquivos gráficos pequenos que podem ser incorporados em suas páginas HTML e que permitem que uma origem não autorizada configure os cookies em seu computador. Esses cookies podem então transmitir as informações para a origem não autorizada.

Por padrão, anúncios, pop-ups e Web bugs são bloqueados em seu computador. Como um Administrador, você pode permitir a exibição de anúncios, pop-ups ou Web bugs sempre que desejar.

Bloquear anúncios

Você pode bloquear a exibição de anúncios quando usuários acessarem a Internet.

Para bloquear anúncios:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Internet & Rede**.
3. Na seção de informações Internet & Rede, clique em **Configurar**.
4. No painel Internet & Configuração de rede, clique em **Avançado** em **Proteção da navegação na Web**.
5. No painel Bloqueio de anúncios, pop-ups & Web bugs, marque a caixa de seleção **Bloquear anúncios que aparecem em páginas da Web quando você navega na Internet**.
6. Clique em **OK**.

Bloquear pop-ups

Você pode bloquear a exibição de pop-ups quando usuários acessarem a Internet.

Para bloquear pop-ups:

1 Em **Tarefas comuns**, clique em **Iniciar**.
2 No painel Início do SecurityCenter, clique em **Internet & Rede**.
3 Na seção de informações Internet & Rede, clique em **Configurar**.
4 No painel Internet & Configuração de rede, clique em **Avançado** em **Proteção da navegação na Web**.
5 No painel Bloqueio de anúncios, pop-ups & Web bugs, marque a caixa de seleção **Bloquear janelas pop-up que aparecem em páginas da Web quando você navega na Internet**.
6 Clique em **OK**.

Bloquear Web bugs

Os Web bugs (também chamados de beacons da Web, marcas de pixel, GIFs de limpeza ou GIFs invisíveis) são arquivos gráficos pequenos que podem ser incorporados em suas páginas HTML e que permitem que uma origem não autorizada configure os cookies em seu computador. Esses cookies podem então transmitir as informações para a origem não autorizada. Você pode evitar que Web bugs sejam carregados no seu computador, bloqueando-os.

Para bloquear Web bugs:

1 Em **Tarefas comuns**, clique em **Iniciar**.
2 No painel Início do SecurityCenter, clique em **Internet & Rede**.
3 Na seção de informações Internet & Rede, clique em **Configurar**.
4 No painel Internet & Configuração de rede, clique em **Avançado** em **Proteção da navegação na Web**.
5 No painel Bloqueio de anúncios, pop-ups & Web bugs, marque a caixa de seleção **Bloquear Web bugs neste computador**.
6 Clique em **OK**.

Bloqueando informações pessoais

Impeça que suas informações pessoais (como nome, endereço, números de cartão de crédito e números de contas bancárias) sejam transmitidas pela Internet, adicionando-as à área de informações bloqueadas. Quando a McAfee detecta informações de identificação pessoal em algo prestes a ser enviado, acontece o seguinte:

- Se você for um administrador, será solicitada sua confirmação para enviar ou não as informações.
- Se você não for um administrador, as informações bloqueadas são substituídas por asteriscos (*). Por exemplo, se você enviar o e-mail *Lance Armstrong ganha o tour* e *Armstrong* estiver definido como uma informação pessoal a ser bloqueada, o e-mail enviado será *Lance ********* ganha o tour*.

Você pode bloquear os seguintes tipos de informações pessoais: nome, endereço, código postal, CPF, número de telefone, números de cartões de crédito, contas bancárias, contas de ações e cartões telefônicos. Se desejar bloquear outros tipos de informações pessoais, você poderá definir esse tipo em **outros**.

Bloquear informações pessoais

Você pode bloquear os seguintes tipos de informações pessoais: nome, endereço, código postal, CPF, número de telefone, números de cartões de crédito, contas bancárias, contas de ações e cartões telefônicos. Se desejar bloquear outros tipos de informações pessoais, você poderá definir esse tipo em **outros**.

Para bloquear informações pessoais:

1. Em **Tarefas comuns**, clique em **Início**.
2. No painel Início do SecurityCenter, clique em **Internet & Rede**.
3. Na seção de informações Internet & Rede, clique em **Configurar**.
4. No painel Configuração de Internet e Rede, assegure-se de que a Proteção de informações pessoais esteja ativada e clique em **Avançado**.
5. No painel Informações bloqueadas, clique em **Adicionar**.
6. Selecione o tipo de informações a serem bloqueadas na lista.
7. Digite suas informações pessoais e clique em **OK**.
8. Na caixa de diálogo Proteção de informações pessoais, clique em **OK**.

CAPÍTULO 36

Protegendo senhas

O Cofre de senhas é uma área segura de armazenamento para suas senhas pessoais. Ele permite que você guarde suas senhas, garantindo que nenhum outro usuário (nem mesmo um Administrador McAfee ou administrador do sistema) poderá acessá-las.

Neste capítulo

Configurando o Cofre de senhas

Antes de começar a usar o Cofre de senhas, você deve definir uma senha para o Cofre de senhas. Apenas usuários que conheçam essa senha poderão acessar seu Cofre de senhas. Se você esquecer a senha do Cofre de senhas, será possível redefini-la; porém, todas as senhas armazenadas anteriormente no Cofre de senhas serão excluídas.

Depois de definir uma senha para o Cofre de senhas, você pode adicionar, editar ou remover senhas de seu cofre.

Adicionar uma senha ao Cofre de senhas

Se tiver problemas para lembrar suas senhas, você poderá adicioná-las ao Cofre de senhas. O Cofre de senhas é um local seguro e só pode ser acessado por usuários que sabem a senha do cofre.

Para adicionar uma senha ao Cofre de senhas:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Internet & Rede**.
3. Na seção de informações Internet & Rede, clique em **Configurar**.
4. No painel Configuração de Internet & rede, clique em **Avançado** em **Proteção de informações pessoais**.
5. No painel Proteção de informações pessoais, clique em **Cofre de senhas**.
6. Digite a senha do Cofre de senhas na caixa **Senha** e digite-a novamente na caixa **Confirmar senha**.
7. Clique em **Abrir**.
8. No painel Cofre de senhas, clique em **Adicionar**.
9. Digite uma descrição da senha (por exemplo, para que ela serve) na caixa **Descrição** e, em seguida, digite a senha na caixa **Senha**.
10. Clique em **Adicionar** e, em seguida, clique em **OK**.

Modificar uma senha no Cofre de senhas

Para garantir que as entradas no Cofre de senhas sejam sempre precisas e confiáveis, é necessário atualizá-las sempre as senhas forem alteradas.

Para modificar uma senha no Cofre de senhas:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Internet & Rede**.
3. Na seção de informações Internet & Rede, clique em **Configurar**.
4. No painel Configuração de Internet & rede, clique em **Avançado** em **Proteção de informações pessoais**.
5. No painel Proteção de informações pessoais, clique em **Cofre de senhas**.
6. Digite a sua senha do Cofre de senhas na caixa **Senha**.
7. Clique em **Abrir**.
8. No painel Cofre de senhas, clique em uma entrada de senha e, em seguida, em **Editar**.
9. Modifique a descrição da senha (por exemplo, para que ela serve) na caixa **Descrição** ou modifique a senha na caixa **Senha**.
10. Clique em **Adicionar** e, em seguida, clique em **OK**.

Remover uma senha do Cofre de senhas

Você pode remover uma senha do Cofre de senhas quando desejar. Não é possível recuperar uma senha removida do cofre.

Para remover uma senha do Cofre de senhas:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Internet & Rede**.
3. Na seção de informações Internet & Rede, clique em **Configurar**.
4. No painel Configuração de Internet & rede, clique em **Avançado** em **Proteção de informações pessoais**.
5. No painel Proteção de informações pessoais, clique em **Cofre de senhas**.
6. Digite a sua senha do Cofre de senhas na caixa **Senha**.
7. Clique em **Abrir**.
8. No painel Cofre de senhas, clique em uma entrada de senha e clique em **Remover**.
9. Na caixa de diálogo Confirmação de remoção, clique em **Sim**.
10. Clique em **OK**.

Redefinir a senha do Cofre de senhas

Se esquecer a senha do Cofre de senhas, você poderá redefini-la; porém, todas as senhas inseridas anteriormente serão excluídas.

Para redefinir a senha do Cofre de senhas:

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Internet & Rede**.
3. No painel de informações Internet & Rede, clique em **Configurar**.
4. No painel Configuração de Internet & rede, clique em **Avançado** em **Proteção de informações pessoais**.
5. No painel Proteção de informações pessoais, clique em **Cofre de senhas**.
6. Em **Redefinir Cofre de senhas**, digite uma nova senha na caixa **Senha** e digite-a novamente na caixa **Confirmar senha**.
7. Clique em **Redefinir**.
8. Na caixa de diálogo Confirmação de redefinição de senha, clique em **Sim**.

CAPÍTULO 37

McAfee Data Backup

Use o Data Backup para evitar a perda acidental de dados, arquivando seus arquivos em unidades de CD, DVD, USB, disco rígido externo ou unidade de rede. O arquivamento local permite que você arquive (faça backup) seus dados pessoais em CD, DVD, unidade USB, disco rígido externo ou unidade de rede. Isso proporciona a você uma cópia local de seus registros, documentos e outros materiais de interesse pessoal em caso de perda acidental.

Antes de começar a usar o Data Backup, você pode se familiarizar com alguns dos recursos mais populares. A Ajuda do Data Backup fornece detalhes sobre como configurar e usar esses recursos. Depois de navegar pelos recursos do programa, você deve assegurar-se de haver mídia para arquivamento adequada disponível para realizar arquivamentos locais.

Neste capítulo

Recursos

O Data Backup fornece os seguintes recursos para salvar e restaurar suas fotos, músicas e outros arquivos importantes.

Arquivamento programado local

Proteja seus dados arquivando arquivos e pastas em CD, DVD, unidade USB, disco rígido externo ou unidade de rede. Depois que você iniciar o primeiro arquivamento, arquivamentos incrementais ocorrerão automaticamente para você.

Restauração em um clique

Se arquivos e pastas forem excluídos por engano ou forem corrompidos em seu computador, você poderá restaurar as versões arquivadas mais recentemente a partir da mídia de arquivamento utilizada.

Compactação e criptografia

Por padrão, seus arquivos arquivados são compactados, economizando espaço na mídia de arquivamento. Como medida adicional de segurança, os arquivos são criptografados por padrão.

CAPÍTULO 38

Arquivando arquivos

Você pode usar o McAfee Data Backup para arquivar uma cópia dos arquivos de seu computador em CD, DVD, unidade USB, unidade de disco rígido externo ou unidade de rede. O arquivamento de seus arquivos dessa maneira facilita a recuperação de informações em caso de dados perdidos ou danificados por acidente.

Antes de começar o arquivamento de arquivos, você deve escolher o local de arquivamento padrão (CD, DVD, unidade USB, disco rígido externo ou unidade de rede). A McAfee pré-configurou algumas outras definições, como os tipos de pastas e arquivos que você deseja arquivar, por exemplo, mas você pode modificar essas configurações.

Depois de definir as opções locais de arquivamento, você pode modificar as configurações padrão para a freqüência com que o Data Backup deve executar arquivamentos completos ou rápidos. Você pode executar arquivamentos manuais a qualquer momento.

Neste capítulo

Configurando opções de arquivamento

Antes de começar a arquivar seus dados, você deve definir algumas opções locais de arquivamento. Por exemplo, você deve definir os locais de observação e os tipos de arquivos observados. Locais de observação são as pastas do computador em que o Data Backup monitora novos arquivos ou alterações nos arquivos. Tipos de arquivos observados são os tipos de arquivos (por exemplo, .doc, .xls e assim por diante) que o Data Backup arquiva dentro dos locais de observação. Por padrão, o Data Backup observa todos os tipos de arquivos armazenados em seu locais de observação.

Você pode definir dois tipos de locais de observação: locais de observação detalhada e locais de observação superficial. Se você definir um local de observação detalhada, o Data Backup arquivará os tipos de arquivos observados dentro dessa pasta e de suas subpastas. Se você definir um local de observação superficial, o Data Backup arquivará os tipos de arquivos observados dentro dessa pasta apenas (não das subpastas). Também é possível identificar locais que você deseje excluir do arquivamento local. Por padrão, a área de trabalho do Windows e Meus documentos são definidos como locais de observação detalhada.

Depois de configurar os tipos e locais dos arquivos observados, você deve configurar o local do arquivamento (isto é, a unidade de CD, DVD, USB, disco rígido externo ou unidade de rede onde os dados arquivados serão armazenados). É possível alterar o local de arquivamento a qualquer momento.

Por motivos de segurança ou problemas de tamanho, a criptografia ou compactação são ativadas por padrão para seus arquivos arquivados. O conteúdo de arquivos criptografados é transformado de texto em código, ocultando as informações para que fiquem ilegíveis para as pessoas que não sabem descriptografá-las. Arquivos compactados são compactados em um formato que minimiza o espaço necessário para armazená-lo ou transmiti-lo. Embora a McAfee não recomende esse procedimento, você pode desativar a criptografia ou a compactação a qualquer momento.

Incluir um local no arquivamento

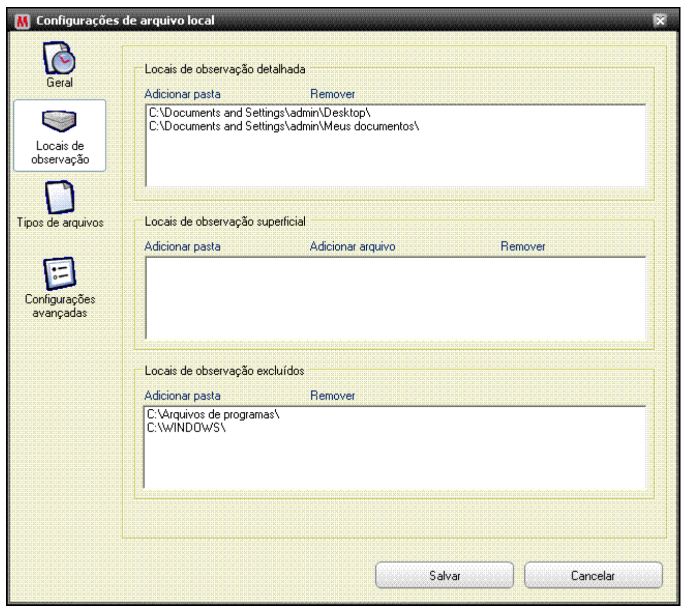
Você pode definir dois tipos de locais de observação para arquivamento: detalhada e superficial. Se você definir um local de observação detalhada, o Data Backup monitorará mudanças no conteúdo da pasta e de suas subpastas. Se você definir um local de observação superficial, o Data Backup monitorará mudanças apenas no conteúdo da pasta (não de suas subpastas).

Para incluir um local no arquivamento:

1 Clique na guia **Arquivamento local**.

2 No painel esquerdo, clique em **Configurações**.

3 Na caixa de diálogo Configurações de arquivo local, clique em **Locais de observação**.



4 Escolha uma das seguintes opções:

- Para arquivar o conteúdo de uma pasta, inclusive o conteúdo de suas subpastas, clique em **Adicionar pasta** em **Locais de observação detalhada**.
- Para arquivar o conteúdo de uma pasta, mas não o conteúdo de suas subpastas, clique em **Adicionar pasta** em **Locais de observação superficial**.

5 Na caixa de diálogo Procurar pasta, navegue até a pasta que deseja observar e clique em **OK**.

6 Clique em **Salvar**.

Dica: Se desejar que o Data Backup observe uma pasta que ainda não foi criada, você pode clicar em **Criar nova pasta**, na caixa de diálogo Procurar pasta, para adicionar uma pasta e defini-la como local de observação ao mesmo tempo.

Definir tipos de arquivo para arquivamento

Você pode especificar que tipos de arquivos devem ser arquivados nos locais de observação detalhada ou superficial. Você pode escolher a partir de uma lista existente de tipos de arquivos ou adicionar um novo tipo à lista.

Para definir tipos de arquivo para arquivamento:

1. Clique na guia **Arquivamento local**.
2. No painel esquerdo, clique em **Configurações**.
3. Na caixa de diálogo Configurações de arquivo local, clique em **Tipos de arquivos**.
4. Expanda as listas de tipos de arquivos e marque as caixas de seleção ao lado dos tipos de arquivos que deseja arquivar.
5. Clique em **Salvar**.

Dica: Para adicionar um novo tipo de arquivo à lista **Tipos de arquivo selecionados**, digite a extensão do arquivo na caixa **Adicionar tipo de arquivo personalizado a 'Outro'** e clique em **Adicionar**. O novo tipo de arquivo se torna automaticamente um tipo de arquivo observado.

Excluir um local do arquivamento

Você pode excluir um local do arquivamento se desejar impedir que esse local (pasta) e seu conteúdo sejam arquivados.

Para excluir um local do arquivamento:

1. Clique na guia **Arquivamento local**.
2. No painel esquerdo, clique em **Configurações**.
3. Na caixa de diálogo Configurações de arquivo local, clique em **Pastas em observação**.
4. Em **Locais de observação excluída**, clique em **Adicionar pasta**.
5. Na caixa de diálogo Procurar pasta, navegue até a pasta que deseja excluir, selecione-a e clique em **OK**.
6. Clique em **Salvar**.

Dica: Se desejar que o Data Backup exclua uma pasta que ainda não foi criada, você pode clicar em **Criar nova pasta**, na caixa de diálogo Procurar pasta, para adicionar uma pasta e excluí-la da observação ao mesmo tempo.

Alterar o local de arquivamento

Quando você altera o local de arquivamento, os arquivos arquivados anteriormente em um local diferente são listados como *Nunca arquivados*.

Para alterar o local de arquivamento:

1 Clique na guia **Arquivamento local**.

2 No painel esquerdo, clique em **Configurações**.

3 Clique em **Alterar local de arquivamento**.

4 Na caixa de diálogo Local do arquivamento, execute uma das seguintes ações:

- Clique em **Selecionar gravador de CD/DVD**, clique na unidade de CD ou DVD de seu computador na lista **Gravador** e clique em **Salvar**.
- Clique em **Selecionar local da unidade**, navegue até uma unidade USB, local ou de disco rígido externo, selecione-a e clique em **OK**.
- Clique em **Selecionar local na rede**, navegue até uma pasta de rede, selecione-a e clique em **OK**.

5 Verifique se o novo arquivamento está em **Local de arquivamento selecionado** e clique em **OK**.

6 Na caixa de diálogo de confirmação, clique em **OK**.

7 Clique em **Salvar**.

Desativar a criptografia e a compactação de arquivos

A criptografia de arquivos arquivados protege a confidencialidade de seus dados, ocultando o conteúdo dos arquivos para que eles fiquem ilegíveis. A compactação de arquivos arquivados ajuda a minimizar o tamanho dos arquivos. Por padrão, a criptografia e a compactação estão ativadas, mas você pode desativar essas opções a qualquer momento.

Para desativar a criptografia e a compactação de arquivos:

1. Clique na guia **Arquivamento local**.
2. No painel esquerdo, clique em **Configurações**.
3. Na caixa de diálogo Configurações de arquivo local, clique em **Configurações avançadas**.
4. Desmarque a caixa de seleção **Ativar criptografia para aumentar a segurança**.
5. Desmarque a caixa de seleção **Ativar compactação para reduzir o armazenamento**.
6. Clique em **Salvar**.

Observação: A McAfee recomenda que você não desative a criptografia e a compactação ao arquivar seus arquivos.

Executando arquivamentos completos e rápidos

Você pode executar dois tipos de arquivamento: completo ou rápido. Ao executar um arquivamento completo, você arquiva um conjunto completo de dados com base nos tipos de arquivos e locais de observação que você configurou. Ao executar um arquivamento rápido, você arquiva apenas os arquivos observados que foram modificados desde o último arquivamento completo ou rápido.

Por padrão, o Data Backup é programado para executar um arquivamento completo dos tipos de arquivos observados em seus locais de observação todas as segundas-feiras às 9 da manhã, e um arquivamento rápido a cada 48 horas depois do último arquivamento completo ou rápido. Essa programação garante que sempre haja um arquivamento atual de seus arquivos. No entanto, se não desejar arquivar a cada 48 horas, você poderá ajustar a programação de acordo com as suas necessidades.

Se desejar arquivar o conteúdo de seus locais de observação sob solicitação, você poderá fazê-lo a qualquer momento. Por exemplo, se você modificar um arquivo e quiser arquivá-lo, mas o Data Backup não estiver programado para executar um arquivamento completo ou rápido nas próximas horas, você pode arquivar manualmente. Quando você arquiva manualmente, o intervalo configurado para arquivamentos automáticos é redefinido.

Você também pode interromper um arquivamento automático ou manual se ele acontecer em um momento inadequado. Por exemplo, se você estiver executando uma tarefa com uso intensivo de recursos e o arquivamento automático for iniciado, você poderá interrompê-lo. Ao interromper um arquivamento automático, o intervalo configurado para arquivamentos automáticos é redefinido.

Programar arquivamentos automáticos

Você pode definir a freqüência dos arquivamentos completos ou automáticos para garantir que seus dados estejam sempre protegidos.

Para programar arquivamentos automáticos:

1. Clique na guia **Arquivamento local**.
2. No painel esquerdo, clique em **Configurações**.
3. Na caixa de diálogo Configurações de arquivo local, clique em **Geral**.
4. Para executar um arquivamento total todos os dias, semanas ou meses, clique em uma das opções a seguir, em **Arquivamento completo a cada**:
   - **Dia**
   - **Semana**
   - **Mês**
5. Marque a caixa de seleção ao lado do dia em que deseja executar o arquivamento completo.
6. Clique em um valor na lista **Às** para especificar o horário em que deseja executar o arquivamento completo.
7. Para executar um arquivamento rápido a cada hora ou todos os dias, clique em uma das opções a seguir, em **Arquivamento rápido**:
   - **Horas**
   - **Dias**
8. Na caixa **Arquivamento rápido a cada**, digite um número que represente a freqüência.
9. Clique em **Salvar**.

Interromper um arquivamento automático

O Data Backup arquiva automaticamente os arquivos dos locais de observação de acordo com a programação que você definir. No entanto, se houver um arquivamento automático em andamento, você poderá interrompê-lo a qualquer momento se desejar.

Para interromper um arquivamento automático:

1. No painel esquerdo, clique em **Parar arquivamento**.
2. Na caixa de diálogo de confirmação, clique em **Sim**.

Observação: O link **Parar arquivamento** aparece apenas quando o arquivamento está em andamento.

Executar arquivamentos manualmente

Embora os arquivamentos automáticos aconteçam de acordo com uma programação predefinida, você pode executar um arquivamento completo ou rápido a qualquer momento. Um arquivamento rápido age apenas nos arquivos modificados desde o último arquivamento completo ou rápido. Um arquivamento completo age sobre os tipos de arquivos em todos os locais de observação.

Para executar um arquivamento rápido ou completo manualmente:

1 Clique na guia **Arquivamento local**.

2 Para executar um arquivamento rápido, clique em **Arquivamento rápido** no painel esquerdo.

3 Para executar um arquivamento completo, clique em **Arquivamento completo** no painel esquerdo.

4 Na caixa de diálogo Pronto para iniciar o arquivamento, verifique o espaço e as configurações de armazenamento e, em seguida, clique em **Continuar**.

CAPÍTULO 39

Trabalhando com arquivos arquivados

Depois de arquivar alguns arquivos, você pode usar o Data Backup para trabalhar com eles. Seus arquivos arquivados são apresentados em uma exibição tradicional de navegador, que permite fácil localização. Conforme seu arquivamento for crescendo, talvez você deseje organizar os arquivos ou procurá-los. Você também pode abrir arquivos diretamente a partir do navegador, para examinar seu conteúdo sem precisar recuperá-los.

Você recupera arquivos de um arquivamento se a cópia local do arquivo estiver desatualizada, ausente ou danificada. O Data Backup também fornece as informações necessárias para gerenciar seus arquivamentos locais e mídias de armazenamento.

Neste capítulo

Usando o navegador de arquivamentos locais

O navegador de arquivamentos locais permite que você exiba e manipule os arquivos arquivados localmente. Você pode exibir o nome, o tipo, o local, o tamanho, o estado (arquivado, não arquivado ou arquivamento em andamento) de cada arquivo, bem como a data do último arquivamento. Também é possível classificar os arquivos por qualquer um desses critérios.

Se houver um arquivamento grande, você poderá encontrar um arquivo rapidamente, fazendo uma pesquisa. Você pode pesquisar o nome completo ou parte do nome ou do caminho do arquivo e restringir sua pesquisa, especificando o tamanho aproximado do arquivo e a data do último arquivamento.

Depois de localizar um arquivo, você pode abri-lo diretamente a partir do navegador de arquivamentos locais. O Data Backup abre o arquivo em seu programa nativo, permitindo que você faça alterações sem sair do navegador de arquivamentos locais. O arquivo é salvo em seu local de observação original no computador e arquivado automaticamente, de acordo com a programação de arquivamento definida.

Classificar arquivos arquivados

Você pode classificar seus arquivos e pastas arquivados de acordo com os critérios a seguir: nome, tipo de arquivo, tamanho, estado (isto é, arquivado, não arquivado ou arquivamento em andamento), a data do último arquivamento ou o local dos arquivos em seu computador (caminho).

Para classificar arquivos arquivados:

1. Clique na guia **Arquivamento local**.
2. No painel direito, clique no nome de uma coluna.

Procurar um arquivo arquivado

Se houver um repositório de arquivamento grande, você poderá encontrar um arquivo rapidamente, fazendo uma pesquisa. Você pode pesquisar o nome completo ou parte do nome do arquivo ou caminho e restringir sua pesquisa, especificando o tamanho aproximado do arquivo e a data do último arquivamento.

Para procurar um arquivo arquivado:

1 Digite o nome completo do arquivo ou parte dele na caixa **Pesquisar** na parte superior da tela e pressione ENTER.

2 Digite o caminho completo ou parte dele na caixa **Caminho completo ou parte**.

3 Especifique o tamanho aproximado do arquivo que está procurando, usando um dos métodos a seguir:
   - Clique em **<100 KB**, **<1 MB** ou **>1 MB**.
   - Clique em **Tamanho em KB** e especifique o tamanho adequado nas caixas.

4 Especifique a data aproximada do último backup on-line do arquivo, usando um dos métodos a seguir:
   - Clique em **Esta semana**, **Este mês** ou **Este ano**.
   - Clique em **Especificar datas**, clique em **Arquivados** na lista e depois clique nas datas apropriadas nas listas de datas.

5 Clique em **Pesquisar**.

Observação: Se você não souber o tamanho ou a data aproximados do último arquivamento, clique em **Desconhecido**.

Abrir um arquivo arquivado

Você pode examinar o conteúdo de um arquivo arquivado abrindo-o diretamente no navegador de arquivamentos locais.

Para abrir arquivos arquivados:

1 Clique na guia **Arquivamento local**.

2 No painel direito, clique em um nome de arquivo e clique em **Abrir**.

Dica: Também é possível abrir um arquivo arquivado clicando duas vezes no nome do arquivo.

Restaurando arquivos arquivados

Se um arquivo observado for danificado, estiver faltando ou for excluído por engano, você poderá restaurar uma cópia dele a partir do arquivamento local. Por isso, é importante assegurar-se de arquivar seus arquivos regularmente. Você também pode restaurar versões anteriores dos arquivos a partir de um arquivamento local. Por exemplo, se você arquiva um arquivo regularmente, poderá retornar para a versão anterior dele, localizando o arquivo no local de arquivamento. Se o local do arquivamento for uma unidade local ou de rede, você pode procurar o arquivo. Se o local do arquivamento for uma unidade de disco rígido externo ou USB, você terá de conectar a unidade ao computador e procurar o arquivo. Se o local do arquivamento for um CD ou DVD, você terá de inserir o CD ou DVD no computador e procurar o arquivo.

Você também pode restaurar arquivos arquivados em um computador a partir de outro computador. Por exemplo, se você arquivar um conjunto de arquivos em um disco rígido externo no computador A, poderá recuperar esses arquivos no computador B. Para isso, você deve instalar o McAfee Data Backup no computador B e conectar o disco rígido externo. Então, no Data Backup, você procura os arquivos e eles são adicionados à lista **Arquivos ausentes** para restauração.

Para obter mais informações sobre arquivamento, consulte Arquivando arquivos. Se desejar excluir propositadamente um arquivo observado de seu arquivamento, você poderá excluir a entrada da lista **Arquivos ausentes**.

Restaurar arquivos ausentes a partir de um arquivamento local

O arquivamento local do Data Backup permite que você recupere dados ausentes de uma pasta observada em seu computador local. Por exemplo, se um arquivo tiver sido removido de uma pasta observada ou excluído e já tiver sido arquivado, você poderá restaurá-lo a partir do arquivamento local.

Para recuperar um arquivo ausente a partir de um arquivamento local:

1. Clique na guia **Arquivamento local**.
2. Na guia **Arquivos ausentes**, na parte inferior da tela, marque a caixa de seleção ao lado do nome do arquivo que deseja restaurar.
3. Clique em **Restaurar**.

Dica: Você pode restaurar todos o arquivos da lista **Arquivos ausentes** clicando em **Restaurar tudo**.

Restaurar uma versão anterior de um arquivo a partir de um arquivamento local

Se desejar restaurar uma versão anterior de um arquivo arquivado, você poderá localizá-lo e adicioná-lo à lista **Arquivos ausentes**. Então, você poderá restaurar o arquivo da mesma maneira que faria com qualquer outro arquivo da lista **Arquivos ausentes**.

Para restaurar uma versão anterior de um arquivo a partir de um arquivamento local:

1 Clique na guia **Arquivamento local**.

2 Na guia **Arquivos ausentes**, na parte inferior da tela, clique em **Procurar** e navegue até o local onde o arquivamento está armazenado.

   Nomes de pastas arquivadas têm o seguinte formato: `cre ddmmaa_hh-mm-ss_***`, onde `ddmmaa` é a data em que os arquivos foram arquivados, `hh-mm-ss` é o horário em que foram arquivados e `***` é `Full` ou `Inc`, conforme o arquivo tenha sido arquivado em arquivamento completo ou rápido.

3 Selecione o local e clique em **OK**.

   Arquivos contidos no local selecionado aparecem na lista **Arquivos ausentes**, prontos para serem restaurados. Para obter mais informações, consulte Restaurar arquivos ausentes a partir de um arquivamento local.

Remover arquivos da lista de arquivos ausentes

Quando um arquivo arquivado é removido de uma pasta observada ou excluído, ele aparece automaticamente na lista **Arquivos ausentes**. Isso avisa você do fato de que há uma inconsistência entre os arquivos arquivados e os arquivos das pastas observadas. Se o arquivo tiver sido removido ou excluído da pasta observada intencionalmente, você poderá excluir o arquivo da lista **Arquivos ausentes**.

Para remover um arquivo da lista de Arquivos ausentes:

1 Clique na guia **Arquivamento local**.

2 Na guia **Arquivos ausentes**, na parte inferior da tela, marque a caixa de seleção ao lado do nome do arquivo que deseja remover.

3 Clique em **Excluir**.

Dica: Você pode remover todos o arquivos da lista **Arquivos ausentes**, clicando em **Excluir tudo**.

Gerenciando arquivos

Você pode exibir um resumo das informações sobre seus arquivamentos completos e rápidos a qualquer momento. Por exemplo, você pode exibir informações sobre a quantidade de dados em observação no momento, a quantidade de dados arquivados e a quantidade de dados em observação que ainda não foram arquivados. Você também pode exibir informações sobre sua programação de arquivamento, tais como a data do último e do próximo arquivamento.

Exibir um resumo de suas atividades de arquivamento

Você pode exibir informações sobre suas atividades de arquivamento a qualquer momento. Por exemplo, você pode exibir a porcentagem de arquivos que foram arquivados, o tamanho dos dados em observação, o tamanho dos dados arquivados e o tamanho dos dados em observação que ainda não foram arquivados. Você também pode exibir a data do último e do próximo arquivamento.

Para exibir um resumo de suas atividades de backup:

1. Clique na guia **Arquivamento local**.
2. No alto da tela, clique em **Resumo da conta**.

CAPÍTULO 40

McAfee EasyNetwork

O McAfee® EasyNetwork ativa o compartilhamento seguro de arquivos, simplifica as transferências de arquivos e automatiza o compartilhamento de impressoras entre computadores de sua rede doméstica.

Antes de começar a usar o EasyNetwork, você pode se familiarizar com alguns dos recursos mais populares. A Ajuda do Easynetwork fornece detalhes sobre como configurar e usar esses recursos.

Neste capítulo

Recursos

O EasyNetwork fornece os recursos a seguir.

Compartilhamento de arquivos

O EasyNetwork facilita o compartilhamento de arquivos entre seu computador e os outros computadores da rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura a esses arquivos. Apenas computadores membros da rede gerenciada (isto é, com acesso total ou administrativo) podem compartilhar arquivos ou acessar arquivos compartilhados por outros membros.

Transferência de arquivos

É possível enviar arquivos a outros computadores que sejam membros da rede gerenciada. Quando você recebe um arquivo, ele aparece em sua caixa de entrada do EasyNetwork. A caixa de entrada é um local de armazenamento temporário para todos os arquivos enviados para você por outros computadores da rede.

Compartilhamento automático de impressoras

Depois que você se associa à rede gerenciada, o EasyNetwork compartilha automaticamente todas as impressoras locais conectadas ao seu computador, usando o nome atual da impressora como nome da impressora compartilhada. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e use essas impressoras.

C A P Í T U L O 4 1

Configurando o EasyNetwork

Antes de usar os recursos do EasyNetwork, você deve iniciar o programa e associar-se à rede gerenciada. Depois de associar-se, você pode decidir sair da rede a qualquer momento.

Neste capítulo

Iniciando o EasyNetwork

Por padrão, você é solicitado a iniciar o EasyNetwork imediatamente depois da instalação; no entanto, você também pode iniciar o EasyNetwork mais tarde.

Iniciar o EasyNetwork

Por padrão, você é solicitado a iniciar o EasyNetwork imediatamente depois da instalação; no entanto, você também pode iniciar o EasyNetwork mais tarde.

Para iniciar o EasyNetwork:

- No menu **Iniciar**, aponte para **Programas**, aponte para **McAfee** e clique em **McAfee EasyNetwork**.

Dica: Se você aceitou criar ícones na área de trabalho e na inicialização rápida durante a instalação, também é possível iniciar o EasyNetwork clicando duas vezes no ícone do McAfee EasyNetwork na área de trabalho ou clicando no ícone do McAfee EasyNetwork na área de notificação à direita da barra de tarefas.

Associando-se a uma rede gerenciada

Depois de instalar o SecurityCenter, um agente de rede é adicionado ao computador e executado em segundo plano. No EasyNetwork, o agente de rede é responsável por detectar uma conexão de rede válida, detectando impressoras locais a serem compartilhadas e monitorando o status da rede.

Se na rede à qual você estiver conectado no momento não for encontrado nenhum outro computador que execute o agente de rede, você será automaticamente transformado em membro da rede e solicitado a identificar se a rede é confiável. Por ser o primeiro computador a associar-se à rede, o nome do seu computador é incluído no nome da rede, mas você poderá renomeá-la quando desejar.

Quando um computador se conecta à rede, uma solicitação de associação é enviada a todos os outros computadores atualmente na rede. A solicitação pode ser concedida por qualquer outro computador com permissões administrativas da rede. O concessor também pode determinar o nível de permissão para o computador que está se associando à rede no momento; por exemplo, convidado (apenas capacidade de transferência de arquivos) ou total/administrativa (capacidade para transferência e compartilhamento de arquivos). No EasyNetwork, computadores com acesso administrativo podem conceder acesso a outros computadores e gerenciar permissões (isto é, promover ou rebaixar computadores); computadores com acesso total não podem executar essas tarefas administrativas. Antes de permitir a associação do computador, é realizado um teste de segurança.

Observação: Depois da associação, se você tiver outros programas de rede da McAfee instalados (o McAfee Wireless Network Security ou o Network Manager, por exemplo), o computador também será reconhecido como membro gerenciado nesses programas. O nível de permissão atribuído a um computador aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o que significam permissões de convidado, total ou administrativa em outros programas de rede da McAfee, consulte a documentação fornecida com o programa.

Associar-se à rede

Quando um computador se conecta a uma rede confiável pela primeira vez depois da instalação do EasyNetwork, uma mensagem pergunta se você deseja se associar à rede gerenciada. Quando o computador concorda em associar-se, uma solicitação é enviada a todos os outros computadores da rede que têm acesso administrativo. Essa solicitação deve ser concedida para que o computador possa compartilhar impressoras e arquivos ou enviar e copiar arquivos da rede. Se o computador for o primeiro computador na rede, ele recebe permissões administrativas automaticamente.

Para associar-se à rede:

1 Na janela Arquivos compartilhados, clique em **Sim, associar à rede agora**.
Quando um computador administrador da rede autorizar sua solicitação, aparecerá uma mensagem perguntando se você deseja permitir que esse computador e os outros computadores da rede gerenciem as configurações de segurança uns dos outros.

2 Para permitir que seu computador e os outros da rede gerenciem as configurações de segurança uns dos outros, clique em **Sim**; caso contrário, clique em **Não**.

3 Confirme se o computador concessor está exibindo as mesmas cartas de baralho que estão sendo exibidas na caixa de diálogo de confirmação de segurança e clique em **Confirmar**.

Observação: Se o computador concessor não exibir as mesmas cartas que são exibidas na caixa de diálogo de confirmação de segurança, houve uma violação de segurança na rede gerenciada. Associar-se à rede poderia colocar seu computador em risco, portanto, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Conceder acesso à rede

Quando um computador solicita associar-se à rede gerenciada, uma mensagem é enviada aos outros computadores da rede que têm acesso administrativo. O primeiro computador a responder à mensagem torna-se o concessor. Como concessor, você é responsável por decidir que tipo de acesso deve ser concedido ao computador: convidado, total ou administrativo.

Para conceder acesso à rede:

1 No alerta, marque uma das caixas de seleção a seguir:

- **Conceder acesso convidado**: Permite que o usuário envie arquivos a outros computadores, mas não compartilhe arquivos.

- **Conceder acesso total para todos os aplicativos gerenciados da rede gerenciada**: Permite que o usuário envie e compartilhe arquivos.
- **Conceder acesso administrativo para todos os aplicativos da rede gerenciada**: Permite que o usuário envie e compartilhe arquivos, conceda acesso a outros computadores e ajuste o nível de permissão de outros computadores.

2 Clique em **Conceder acesso**.

3 Confirme se o computador está exibindo as mesmas cartas de baralho que estão sendo exibidas na caixa de diálogo de confirmação de segurança e clique em **Confirmar**.

Observação: Se o computador não exibir as mesmas cartas que estão sendo exibidas na caixa de diálogo de confirmação de segurança, houve uma violação de segurança na rede gerenciada. Conceder acesso à rede para esse computador pode colocar seu computador em risco, portanto, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Renomear a rede

Por padrão, o nome da rede inclui o nome do primeiro computador associado, mas você pode mudar o nome da rede a qualquer momento. Ao renomear a rede, você muda a descrição dela exibida no EasyNetwork.

Para renomear a rede:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, digite o nome da rede na caixa **Nome da rede**.
3. Clique em **OK**.

Saindo de uma rede gerenciada

Se você se associar a uma rede gerenciada e depois decidir que não quer mais ser um membro, é possível deixar a rede. Depois de renunciar à sua associação, você pode se associar novamente a qualquer momento, mas será preciso receber permissão para associar-se e executar a verificação de segurança novamente. Para obter mais informações, consulte Associando-se a uma rede gerenciada (página 277).

Sair de uma rede gerenciada

Você pode sair da rede gerenciada à qual se associou anteriormente.

Para sair de uma rede gerenciada:

1 No menu **Ferramentas**, clique em **Sair da rede**.

2 Na caixa de diálogo Sair da rede, selecione o nome da rede da qual deseja sair.

3 Clique em **Sair da rede**.

CAPÍTULO 42

Compartilhando e enviando arquivos

O EasyNetwork facilita o compartilhamento e o envio de arquivos entre seu computador e os outros computadores da rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura a esses arquivos. Apenas computadores membros da rede gerenciada (isto é, com acesso total ou administrativo) podem compartilhar arquivos ou acessar arquivos compartilhados por outros computadores-membros.

Neste capítulo

Compartilhando arquivos

O EasyNetwork facilita o compartilhamento de arquivos entre seu computador e os outros computadores da rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura a esses arquivos. Apenas computadores membros da rede gerenciada (isto é, com acesso total ou administrativo) podem compartilhar arquivos ou acessar arquivos compartilhados por outros computadores-membros. Se você compartilhar uma pasta, todos os arquivos da pasta e suas subpastas serão compartilhados, mas arquivos adicionados posteriormente à pasta não serão compartilhados automaticamente. Se uma pasta ou um arquivo compartilhado for excluído, será imediatamente removido da janela Arquivos compartilhados. É possível parar de compartilhar arquivos a qualquer momento.

Você pode acessar arquivos compartilhados de duas maneiras: abrindo o arquivo diretamente a partir do EasyNetwork ou copiando o arquivo para um local em seu computador e abrindo-o em seguida. Se sua lista de arquivos compartilhados ficar longa, você poderá procurar os arquivos compartilhados que deseja acessar.

Observação: Arquivos compartilhados através do EasyNetwork não podem ser acessados a partir de outros computadores por meio do Windows Explorer. O compartilhamento de arquivos do EasyNetwork é realizado em conexões seguras.

Compartilhar um arquivo

Quando você compartilha um arquivo, ele se torna automaticamente disponível para todos os outros membros com acesso total ou administrativo à rede gerenciada.

Para compartilhar um arquivo:

1. No Windows Explorer, localize o arquivo que deseja compartilhar.
2. Arraste o arquivo de seu local no Windows Explorer até a janela Arquivos compartilhados no EasyNetwork.

Dica: Você também pode compartilhar um arquivo clicando em **Compartilhar arquivos** no menu **Ferramentas**. Na caixa de diálogo Compartilhar, navegue até a pasta em que está armazenado o arquivo que deseja compartilhar e clique em **Compartilhar**.

Parar de compartilhar um arquivo

Se você compartilhar um arquivo na rede gerenciada, poderá parar de compartilhá-lo a qualquer momento. Quando você para de compartilhar um arquivo, os outros membros da rede gerenciada não podem mais acessá-lo.

Para parar de compartilhar um arquivo:

1. No menu **Ferramentas**, clique em **Deixar de compartilhar arquivos**.
2. Na caixa de diálogo Deixar de compartilhar arquivos, selecione o arquivo que não deseja mais compartilhar.
3. Clique em **Não compartilhar**.

Copiar um arquivo compartilhado

Você pode copiar arquivos compartilhados de qualquer computador da rede gerenciada para o seu computador. Depois, se o computador parar de compartilhar o arquivo, você ainda terá uma cópia.

Para copiar um arquivo:

- Arraste um arquivo da janela Arquivos compartilhados do EasyNetwork para um local no Windows Explorer ou para a área de trabalho do Windows.

Dica: Você também pode copiar um arquivo compartilhado selecionando o arquivo no EasyNetwork e clicando em **Copiar para** no menu **Ferramentas**. Na caixa de diálogo Copiar para, navegue até a pasta para a qual deseja copiar o arquivo, selecione-a e clique em **Salvar**.

Procurar um arquivo compartilhado

Você pode procurar um arquivo que foi compartilhado por você ou por qualquer outro membro da rede. Enquanto você digita os critérios de pesquisa, o EasyNetwork exibe automaticamente os resultados correspondentes na janela Arquivos compartilhados.

Para procurar um arquivo compartilhado:

1. Na janela Arquivos compartilhados, clique em **Pesquisar**.
2. Clique em uma das opções a seguir, na lista **Contém**:
   - **Contém todas as palavras**: Procura todos os nomes de arquivos ou caminhos que contenham todas as palavras especificadas na lista **Nome do arquivo ou caminho**, em qualquer ordem.

- **Contém qualquer uma das palavras**: Pesquisa nomes de arquivos ou caminhos que contenham qualquer uma das palavras especificadas na lista **Nome do arquivo ou caminho**.
- **Contém a seqüência de caracteres exata**: Procura nomes de arquivos ou caminhos que contenham a frase exata especificada na lista **Nome do arquivo ou caminho**.

3 Digite uma parte ou todo o nome do arquivo ou caminho na lista **Nome do arquivo ou caminho**.

4 Clique em um dos tipos de arquivos a seguir, na lista **Tipo**:

- **Qualquer**: Pesquisa todos os tipos de arquivos compartilhados.
- **Documento**: Pesquisa todos os documentos compartilhados.
- **Imagem**: Pesquisa todos os arquivos de imagem compartilhados.
- **Vídeo**: Pesquisa todos os arquivos de vídeo compartilhados.
- **Áudio**: Pesquisa todos os arquivos de áudio compartilhados.

5 Nas listas **De** e **Até**, clique em datas que representem o intervalo de datas durante o qual o arquivo foi criado.

Enviando arquivos para outros computadores

É possível enviar arquivos a outros computadores que sejam membros da rede gerenciada. Antes de enviar um arquivo, o EasyNetwork confirma se o computador de destino tem espaço em disco disponível suficiente.

Quando você recebe um arquivo, ele aparece em sua caixa de entrada do EasyNetwork. A caixa de entrada é um local de armazenamento temporário para todos os arquivos enviados para você por outros computadores da rede. Se o EasyNetwork estiver aberto no momento em que você recebe um arquivo, o arquivo aparece instantaneamente em sua caixa de entrada. Caso contrário, aparecerá uma mensagem na área de notificação à direita da barra de tarefas do Windows. Se não desejar receber mensagens de notificação, você pode desligá-las. Se um arquivo com o mesmo nome já existir na caixa de entrada, o novo arquivo é renomeado com um sufixo numérico. Os arquivos permanecem em sua caixa de entrada até que você os aceite (isto é, copie-os para um local em seu computador).

Enviar um arquivo para outro computador

Você pode enviar um arquivo diretamente para outro computador na rede gerenciada, sem compartilhá-lo. Para que um usuário no computador de destino possa exibir o arquivo, este deve ser salvo localmente. Para obter mais informações, consulte Aceitar um arquivo de outro computador (página 288).

Para enviar um arquivo para outro computador:

1. No Windows Explorer, localize o arquivo que deseja enviar.
2. Arraste o arquivo de seu local no Windows Explorer até um ícone de um computador ativo no EasyNetwork.

Dica: Você pode enviar diversos arquivos para um computador, pressionando CTRL ao selecionar os arquivos. Também é possível enviar os arquivos clicando em **Enviar** no menu **Ferramentas**, selecionando os arquivos e, em seguida, clicando em **Enviar**.

Aceitar um arquivo de outro computador

Se outro computador da rede gerenciada enviar um arquivo para você, você deverá aceitá-lo (salvando-o em uma pasta do seu computador). Se o EasyNetwork não estiver aberto ou em primeiro plano quando o arquivo for enviado para o computador, você receberá uma mensagem de notificação na área de notificação à direita da barra de tarefas. Clique na mensagem de notificação para abrir o EasyNetwork e acessar o arquivo.

Para receber um arquivo de outro computador:

- Clique em **Recebido** e arraste o arquivo da caixa de entrada do EasyNetwork para uma pasta no Windows Explorer.

Dica: Você também pode receber um arquivo de outro computador selecionando o arquivo na caixa de entrada do EasyNetwork e clicando em **Aceitar** no menu **Ferramentas**. Na caixa de diálogo Aceitar, navegue até a pasta em que deseja salvar os arquivos recebidos, selecione-a e clique em **Salvar**.

Receber uma notificação quando um arquivo for enviado

É possível receber uma notificação quando outro computador da rede gerenciada enviar um arquivo. Se o EasyNetwork não estiver aberto no momento ou não estiver em primeiro plano em sua área de trabalho, uma mensagem de notificação aparecerá na área de notificação, à direita da barra de tarefas do Windows.

Para receber uma notificação quando um arquivo for enviado:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, marque a caixa de seleção **Notificar quando algum outro computador enviar arquivos para mim**.
3. Clique em **OK**.

CAPÍTULO 43

Compartilhando impressoras

Depois que você se associa à rede gerenciada, o EasyNetwork compartilha automaticamente todas as impressoras locais conectadas ao seu computador. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e use essas impressoras.

Neste capítulo

Trabalhando com impressoras compartilhadas

Depois que você se associa à rede gerenciada, o EasyNetwork compartilha automaticamente todas as impressoras locais conectadas ao seu computador, usando o nome atual da impressora como nome da impressora compartilhada. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e use essas impressoras. Se você tiver configurado um driver de impressora para imprimir através de um servidor de impressão da rede (por exemplo, um servidor de impressão USB sem fio), o EasyNetwork considerará essa impressora como uma impressora local e a compartilhará automaticamente na rede. Também é possível parar de compartilhar uma impressora a qualquer momento.

O EasyNetwork também detecta impressoras compartilhadas por todos os outros computadores da rede. Se ele detectar uma impressora remota que ainda não esteja conectada ao seu computador, o link **Impressoras de rede disponíveis** aparecerá na janela Arquivos compartilhados quando você abrir o EasyNetwork pela primeira vez. Isso permite que você instale as impressoras disponíveis ou desinstale impressoras que já estejam conectadas ao seu computador. Também é possível atualizar a lista de impressoras detectadas na rede.

Se você ainda não se associou à rede gerenciada, mas está conectado a ela, é possível acessar as impressoras compartilhadas a partir do painel de controle padrão do Windows.

Parar de compartilhar uma impressora

É possível parar de compartilhar uma impressora a qualquer momento. Membros que instalaram a impressora não poderão mais imprimir com ela.

Para parar de compartilhar uma impressora:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Gerenciar impressoras da rede, clique no nome da impressora que não deseja mais compartilhar.
3. Clique em **Não compartilhar**.

Instalar uma impressora de rede disponível

Como membro de uma rede gerenciada, você pode acessar as impressoras compartilhadas na rede. Para fazer isso, instale o driver usado pela impressora. Se o proprietário da impressora parar de compartilhá-la depois da instalação, você não poderá mais imprimir com essa impressora.

Para instalar uma impressora de rede disponível:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Impressoras de rede disponíveis, clique em um nome de impressora.
3. Clique em **Instalar**.

CAPÍTULO 44

Referência

O Glossário de termos lista e define a terminologia de segurança usada com mais freqüência nos produtos McAfee.

A seção Sobre a McAfee fornece informações legais sobre a McAfee Corporation.

Glossário

8

802.11

Um conjunto de padrões IEEE para tecnologia de LAN sem fio. O 802.11 especifica uma comunicação pelo ar entre um cliente sem fio e uma estação base ou entre dois clientes sem fio. As várias especificações do 802.11 são: 802.11a, um padrão para comunicação em rede até 54 Mbps na banda de 5 Ghz; 802.11b, um padrão para rede até 11 Mbps na banda de 2,4 Ghz; 802.11g, um padrão para rede até 54 Mbps na banda de 2,4 Ghz; e 802.11i, um conjunto de padrões de segurança para todas as redes Ethernet sem fio.

802.11a

Uma extensão do 802.11 que se aplica a LANs sem fio e que envia dados a até 54 Mbps na banda de 5 GHz. Embora a velocidade de transmissão seja maior do que com o 802.11b, o alcance é muito menor.

802.11b

Uma extensão do 802.11 que se aplica a LANs sem fio e que permite transmissão a 11 Mbps na banda de 2,4 GHz. O 802.11b é considerado atualmente o padrão em comunicação sem fio.

802.11g

Uma extensão do 802.11 que se aplica a LANs sem fio e que permite até 54 Mbps na banda de 2,4 GHz.

802.1x

Não suportado pelo Wireless Home Network Security. Um padrão IEEE para autenticação em redes com ou sem fio, porém mais freqüentemente usado em conjunto com a rede sem fio 802.11. Esse padrão proporciona uma autenticação forte e mútua entre um cliente e um servidor de autenticação. Além disso, o 802.1x pode fornecer chaves WEP dinâmicas por usuário e por sessão, eliminando o trabalho administrativo e os riscos de segurança inerentes às chaves WEP estáticas.

A

adaptador sem fio

Contém os circuitos necessários para que um computador ou outro dispositivo se comunique com um roteador sem fio (conectado a uma rede sem fio). Os adaptadores sem fio podem ser incorporados nos circuitos principais de um dispositivo de hardware ou podem ser uma extensão avulsa a ser inserida em um dispositivo através da porta apropriada.

Análise de imagens

Impede que imagens potencialmente inapropriadas apareçam. As imagens são bloqueadas para todos os usuários, exceto membros da faixa etária adulta.

arquivamento completo

Arquivar um conjunto completo de dados com base nos tipos de arquivos e locais de observação que você configurou.

arquivamento rápido

Arquivar apenas os arquivos em observação que foram alterados desde o último arquivamento rápido ou completo.

arquivar

Criar uma cópia dos seus arquivos observados localmente na unidade USB, de CD, de DVD, de disco rígido externo ou de rede.

arquivar

Criar uma cópia dos seus arquivos observados localmente na unidade USB, de CD, de DVD, de disco rígido externo ou de rede.

ataque de dicionário

Esses ataques envolvem a tentativa de uma variedade de palavras de uma lista para descobrir a senha de alguém. Os atacantes não experimentam manualmente todas as combinações, mas possuem ferramentas que tentam automaticamente identificar uma senha.

ataque de força bruta

Também conhecido como cracking por força bruta, trata-se de um método de tentativa e erro utilizado por programas aplicativos para decodificar dados criptografados, como senhas, através de procedimentos exaustivos (ou seja, força bruta) em vez de empregar estratégias intelectuais. Assim como um criminoso pode abrir ou arrombar um cofre tentando várias combinações possíveis, um aplicativo de crack força bruta experimenta seqüencialmente todas as combinações possíveis de caracteres válidos. A força bruta é considerada uma abordagem infalível, embora demorada.

ataque man-in-the-middle (homem no meio)

O atacante intercepta mensagens em uma troca de chaves públicas e, em seguida, as retransmite, substituindo a chave requisitada pela sua própria chave pública, de maneira que as duas partes originais ainda pareçam estar se comunicando diretamente uma com a outra. O atacante usa um programa que aparenta ser o servidor para o cliente e que aparenta ser o cliente para o servidor. Esse ataque pode ser usado simplesmente para obter acesso às mensagens ou para permitir ao atacante modificá-las antes de retransmiti-las. O termo é derivado do jogo de bola no qual algumas pessoas tentam jogar uma bola diretamente de uma para outra enquanto uma pessoa no meio tenta alcançá-la.

autenticação

O processo de identificação de um indivíduo, normalmente com base em um nome de usuário e uma senha. A autenticação garante que o indivíduo é quem afirma ser, mas nada diz quanto aos direitos de acesso desse indivíduo.

B

backup

Criar uma cópia dos seus arquivos observados em um servidor on-line seguro.

biblioteca

A área de armazenamento on-line para os arquivos publicados pelos usuários do Data Backup. A biblioteca é um site na Internet, acessível a todos que tenham acesso à Internet.

C

cabeçalho

Cabeçalho são informações adicionadas à parte da mensagem em todo o seu ciclo de vida. O cabeçalho informa ao software de Internet como enviar a mensagem, para onde as respostas da mensagem devem ser enviadas, um identificador exclusivo para a mensagem de e-mail e outras informações administrativas. Exemplos de campos de cabeçalho: Para, De, CC, Data, Assunto, ID de mensagem e Recebido.

cavalo de Tróia

Os cavalos de Tróia são programas que fingem ser aplicativos benignos. Os cavalos de Tróia não são vírus porque não se replicam, mas podem ser tão destruidores quanto os vírus.

chave

Uma série de letras e/ou números usados por dois dispositivos para autenticar sua comunicação. Ambos os dispositivos precisam ter a chave. Consulte também WEP, WPA, WPA2, WPA-PSK e WPA2-PSK.

cliente

Um aplicativo, executado em um computador pessoal ou estação de trabalho, que depende de um servidor para executar algumas operações. Por exemplo, um cliente de e-mail é um aplicativo que permite enviar e receber e-mail.

cliente de e-mail

Uma conta de e-mail. Por exemplo, Microsoft Outlook ou Eudora.

Cofre de senhas

Uma área de armazenamento segura para suas senhas pessoais. Ele permite que você guarde suas senhas, garantindo que nenhum outro usuário (nem mesmo um Administrador McAfee ou administrador do sistema) poderá acessá-las.

compactação

Um processo através do qual os dados (arquivos) são compactados em um formato que minimiza o espaço necessário para armazená-lo ou transmiti-lo.

compartilhar

Uma operação que permite que os destinatários de e-mail acessem os arquivos com backup selecionados, por um período limitado. Ao compartilhar um arquivo, você envia a cópia de backup do arquivo para os destinatários de e-mail especificados. Os destinatários recebem uma mensagem de e-mail do Data Backup, indicando que os arquivos foram compartilhados com eles. O e-mail também contém um link para os arquivos compartilhados.

conta de e-mail padrão

A maioria dos usuários domésticos usa este tipo de conta. Consulte também conta POP3.

conta MAPI

Acrônimo para Messaging Application Programming Interface (interface de programação de aplicativos de mensagens). A especificação de interface da Microsoft que permite que diferentes aplicativos de mensagens e de grupos de trabalho (incluindo e-mail, correio de voz ou fax) funcionem através de um único cliente, como o cliente Exchange. Por isso, normalmente o MAPI é usado em ambientes corporativos quando a empresa possui o Microsoft® Exchange Server. Porém, muitas pessoas usam o Microsoft Outlook como e-mail pessoal da Internet.

conta MSN

Acrônimo para Microsoft Network. Um serviço on-line e portal de Internet. Essa é uma conta com base na Web.

conta POP3

Acrônimo para Post Office Protocol 3. A maioria dos usuários domésticos possuem esse tipo de conta. Essa é a versão atual do padrão Post Office Protocol em uso comum nas redes TCP/IP. Também conhecida como conta de e-mail padrão.

controles pelos pais

Configurações que permitem que você configure as classificações de conteúdo, que restringem os sites e o conteúdo que um usuário pode exibir, bem como os limites de horário da Internet, que especificam o período e a duração do horário em que um usuário pode acessar a Internet. Eles também permitem que você restrinja universalmente o acesso a sites da Web específicos, além de conceder e bloquear o acesso com base em faixa etária e palavras-chave associadas.

cookie

Na World Wide Web, um bloco de dados que um servidor Web armazena em um sistema do cliente. Quando um usuário retorna ao mesmo site da Web, o navegador envia uma cópia do cookie de volta para o servidor. Os cookies são usados para identificar usuários, instruir o servidor a enviar uma versão personalizada da página da Web solicitada, submeter informações da conta para o usuário, e para outras finalidades administrativas.

Os cookies permitem que o sites memorizem quem é você e controlem quantas pessoas visitaram o site, quando visitaram e quais páginas foram exibidas. Os cookies também ajudam uma empresa a personalizar seu site da Web. Muitos sites da Web exigem um nome de usuário e senha para o acesso a determinadas páginas, e enviam um cookie ao seu computador para que você não precise fazer logon a cada visita. No entanto, os cookies podem ser usados com fins maliciosos. As empresas de propaganda on-line freqüentemente usam cookies para determinar quais sites você visita com mais freqüência e colocam anúncios em seus sites favoritos. Antes de aceitar os cookies de um site, verifique se ele é confiável.

Embora sejam uma fonte de informações para empresas legítimas, os cookies também podem ser uma fonte de informações para hackers. Muitos sites com lojas on-line armazenam informações de cartões de crédito e outras informações pessoais em cookies para facilitar as compras. Infelizmente, pode haver falhas de segurança que permitam o acesso dos hackers às informações dos cookies armazenados nos computadores dos clientes.

criptografia

Um processo através do qual os dados são transformados de texto para código, ocultando as informações para que fiquem ilegíveis para as pessoas que não sabem descriptografá-las.

D

disco rígido externo

Uma unidade de disco rígido é armazenada fora do gabinete do computador.

DNS

Acrônimo para Domain Name System (sistema de nomes de domínios). O sistema hierárquico através do qual os hosts na Internet possuem endereços de nome de domínio (como bluestem.prairienet.org) e endereços IP (como 192.17.3.4). O endereço de nome de domínio é usado por usuários humanos e é automaticamente convertido no endereço IP numérico, que é usado pelo software de roteamento de pacotes. Os nomes DNS consistem em um domínio de nível superior (como: .com, .org e .net), um domínio de nível secundário (o nome do site de uma empresa, organização ou indivíduo), e possivelmente um ou mais subdomínios (servidores dentro de um domínio de nível secundário). Consulte também servidor DNS e endereço IP.

domínio

Um endereço de uma conexão de rede que identifica o proprietário desse endereço em um formato hierárquico: server.organization.type. Por exemplo, www.whitehouse.gov identifica o servidor da Web na Casa Branca, que faz parte do governo dos EUA.

E

e-mail

Correio eletrônico, mensagens enviadas através da Internet ou dentro de uma LAN ou WAN corporativa. Anexos de e-mail na forma de arquivos executáveis (EXE) ou VBS (scripts Visual Basic) tornaram-se muito populares como forma de transmissão de vírus e cavalos de Tróia.

Endereço IP

O endereço Internet Protocol ou o endereço IP é um número exclusivo composto por quatro partes separadas por pontos (p. ex. 63.227.89.66). Todos os computadores da Internet, dos maiores servidores a um laptop, que se comunicam através de um telefone celular, têm um número IP exclusivo. Nem todos os computadores têm um nome de domínio, mas todos têm um IP.

Os itens a seguir listam alguns tipos de endereço IP incomuns:

- Endereços IP não roteáveis: Também conhecidos como Espaço IP privado. São endereços IP que não podem ser usados na Internet. Os blocos de endereços IP privados são 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.
- Endereços IP de Loopback**:** Os endereços de loopback são usados para teste. O tráfego enviado a esse bloco de endereços IP volta para o dispositivo que gerou o pacote. Ele

nunca sai do dispositivo, sendo usado principalmente para testes de hardware e software. O bloco de endereços IP de loopback é 127.x.x.x.

Endereço IP nulo: É um endereço IP inválido. Quando visualizado, ele indica que o tráfego tinha um endereço IP em branco. Obviamente, isso não é normal e geralmente indica que o remetente está escondendo a origem do tráfego. O remetente não poderá receber nenhuma resposta para esse tráfego, a não ser que o pacote seja recebido por um aplicativo que reconheça seu conteúdo e que o pacote contenha instruções específicas para esse aplicativo. Qualquer endereço iniciado com 0 (0.x.x.x) é um endereço nulo. Por exemplo, 0.0.0.0 é um endereço IP nulo.

Endereço MAC (Media Access Control)

Um endereço de baixo nível atribuído ao dispositivo físico que acessa a rede.

ESS (Extended Service Set)

Um conjunto de duas ou mais redes que formam uma única sub-rede.

estação

Um único computador conectado a uma rede.

evento

Eventos de 0.0.0.0

Se você vir eventos de endereços IP 0.0.0.0, há duas possíveis causas. A primeira, e mais comum, é que por algum motivo o computador recebeu um pacote mal formatado. A Internet não é cem por cento confiável, e podem ocorrer pacotes ruins. Como o Firewall vê os pacotes antes que o TCP/IP possa validá-los, ele pode relatar esses pacotes como um evento.

A segunda situação ocorre quando o IP de origem é fraudado ou falso. Pacotes fraudados podem ser um sinal de que alguém está procurando por cavalos de Tróia e tentou fazê-lo em seu computador. É importante se lembrar de que o Firewall bloqueia a tentativa.

Eventos de 127.0.0.1

Às vezes, os eventos indicam o IP de origem como 127.0.0.1. É importante observar que esse IP é especial e é conhecido como endereço de loopback.

Independentemente de qual computador você esteja usando, 127.0.0.1 sempre se refere ao seu computador local. Esse endereço também é chamado de host local, pois o host local de nome de computador sempre será convertido novamente no endereço IP 127.0.0.1. Isso significa que o computador está tentando invadir ele mesmo? Algum Cavalo de Tróia ou spyware está tentando tomar o controle de seu computador? Provavelmente não. Muitos programas legítimos usam o endereço de loopback para comunicação entre componentes. Por exemplo, muitos servidores de e-mail pessoal ou servidores Web podem ser configurados através de uma interface da Web que geralmente é acessada através de um endereço semelhante a http://localhost/.

Contudo, o Firewall permite o tráfego desses programas; portanto, se você vir eventos de 127.0.0.1, isso geralmente significa que o endereço IP de origem foi fraudado ou é falso. Os pacotes fraudados geralmente são um sinal de que alguém está fazendo uma varredura em busca de Cavalos de Tróia. É importante se lembrar de que o Firewall bloqueia essa tentativa. Evidentemente, relatar eventos de 127.0.0.1 não será útil; portanto, não há necessidade de tal procedimento.

Assim sendo, alguns programas, particularmente o Netscape 6.2 e posteriores, exigem que o endereço 127.0.0.1 seja adicionado à lista **Endereços IP confiáveis**. Os componentes desses programas se comunicam entre si de uma maneira que impede que o Firewall determine se o tráfego é local.

No exemplo do Netscape 6.2, se você não confiar no 127.0.0.1, não poderá usar a sua lista de amigos. Portanto, se você receber tráfego de 127.0.0.1 e todos os programas do computador funcionarem normalmente, é sinal de que esse tráfego pode ser bloqueado sem problemas. No entanto, se um programa (como o Netscape) estiver com problemas, adicione 127.0.0.1 à lista **Endereços IP confiáveis** no Firewall e, em seguida, veja se o problema foi resolvido.

Se a inserção de 127.0.0.1 na lista **Endereços IP confiáveis** corrigir o problema, será necessário considerar as seguintes opções: se confiar no 127.0.0.1, o programa funcionará, mas você estará mais vulnerável a ataques de fraude. Se você não confiar no endereço, o programa não funcionará, mas você continuará protegido contra qualquer tráfego mal-intencionado.

Eventos de computadores na LAN

Para a maioria das configurações de LAN corporativas, você pode confiar em todos os computadores na sua LAN.

Eventos de endereços IP privados

Os endereços IP de formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 são chamados de não-roteáveis ou privados. Esses endereços IP nunca devem sair da sua rede e, na maioria das vezes, são confiáveis.

O bloco 192.168 é usado com o Microsoft Internet Connection Sharing (ICS). Se você estiver usando ICS e vir eventos desse bloco de IP, poderá adicionar o endereço IP 192.168.255.255 à sua lista **Endereços IP confiáveis**. Isso tornará todo o bloco 192.168.xxx.xxx confiável.

Se você não estiver em uma rede privada e receber eventos desses intervalos de endereços IP, talvez o endereço IP de origem seja fraudado ou falso. Pacotes fraudados são, em geral, sinal de que alguém está em busca de cavalos de Tróia. É importante se lembrar de que o Firewall bloqueia essa tentativa.

Como os endereços IP privados são separados dos endereços IP da Internet, relatar esses eventos não causa nenhum efeito.

falsificação de IP

Consiste em forjar o endereço IP de um pacote IP. Isso é usado em diversos tipos de ataque, incluindo seqüestro de sessão. Também é freqüentemente utilizado para falsificar os cabeçalhos de e-mail de SPAM para impedir que sejam rastreados corretamente.

firewall

Um sistema desenvolvido para impedir o acesso não autorizado a uma rede privada ou a partir de uma rede privada. Os firewalls podem ser implementados tanto em hardware quanto em software, ou como uma combinação de ambos. Firewalls são freqüentemente utilizados para impedir usuários da Internet não autorizados de acessarem redes privadas conectadas à Internet, especialmente intranets. Todas as mensagens que entram e que saem da intranet passam pelo firewall. O firewall examina cada mensagem e bloqueia as que não satisfazem os critérios de segurança especificados. O firewall é considerado a primeira linha de defesa na proteção de informações privadas. Para maior segurança, os dados podem ser criptografados.

gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (PA), roteador e firewall. Alguns dispositivos também podem incluir aperfeiçoamentos de segurança e recursos de ponte.

grupos de classificação de conteúdo

Faixa etária à qual um usuário pertence. O conteúdo é classificado (ou seja, disponibilizado ou bloqueado) com base no grupo de classificação de conteúdo ao qual o usuário pertence. Os grupos de classificação de conteúdo incluem: crianças pequenas, crianças, pré-adolescentes, adolescentes e adultos.

hotspot

Um local físico específico no qual um ponto de acesso (PA) oferece serviços públicos de rede sem fio em banda larga para visitantes móveis através de uma rede sem fio. Os hotspots costumam estar situados em locais com alta concentração de pessoas, como aeroportos, estações de trens, bibliotecas, marinas, centros de convenções e hotéis. Eles normalmente têm um alcance curto.

Internet

A Internet é composta por um grande número de redes interconectadas que usam protocolos TCP/IP para a localização e a transferência de dados. A Internet surgiu como uma rede criada para ligar computadores de universidades e faculdades (no fim da década de 60 e começo de 70), fundada pelo Departamento de Defesa dos EUA e era chamada ARPANET. A Internet hoje é uma rede global de quase 100.000 redes independentes.

intranet

Uma rede privada, geralmente dentro de uma organização, que funciona de forma muito semelhante à Internet. Agora é prática comum conceder acesso às intranets para computadores independentes usados por alunos ou funcionários remotos. Firewalls, procedimentos de logon e senhas são usados para oferecer segurança.

LAN (Local Area Network)

Uma rede de computadores que se estende por uma área relativamente pequena. A maioria das LANs se restringe a um mesmo edifício ou grupo de edifícios. No entanto, uma LAN pode ser conectada a outras LANs a qualquer distância, via telefone ou ondas de rádio. Um sistema de LANs conectadas dessa forma é o que se chama de rede de longa distância (WAN, wide-area network). A maioria das LANs conectam estações de trabalho e computadores pessoais, geralmente através de hubs ou switches simples. Cada nó (computador individual) de uma LAN possui sua própria CPU, com a qual executa programas, mas também é capaz de acessar dados e dispositivos (como, por exemplo, impressoras) em qualquer lugar da LAN. Isso significa que vários usuários podem compartilhar dispositivos caros, como impressoras a laser, bem como dados. Os usuários também podem usar a LAN para se comunicar uns com os outros, por exemplo, enviando e-mail ou entrando em sessões de chat.

largura de banda

A quantidade de dados que podem ser transmitidos em um determinado período de tempo. Em dispositivos digitais, a largura de banda costuma ser expressa em bits por segundo (bps) ou em bytes por segundo. Em dispositivos analógicos, a largura de banda é expressa em ciclos por segundo ou Hertz (Hz).

lista branca

Uma lista de sites da Web que possuem permissão para serem acessados, por não serem considerados fraudulentos.

lista negra

Uma lista de sites da Web considerados mal intencionados. Um site da Web pode ser colocado em uma lista negra por ser uma operação fraudulenta ou por explorar a vulnerabilidade do navegador para enviar programas potencialmente indesejados ao usuário.

locais de observação

As pastas no seu computador monitoradas pelo Data Backup.

locais de observação superficial

Uma pasta em seu computador na qual as alterações são monitoradas pelo Data Backup. Se você configurar um local de observação superficial, o Data Backup fará backup dos tipos de arquivos em observação dentro dessa pasta, mas não incluirá suas subpastas.

local de observação detalhada

Uma pasta (e todas as subpastas) em seu computador na qual as alterações são monitoradas pelo Data Backup. Se você definir um local de observação detalhada, o Data Backup fará backup dos tipos de arquivos em observação dentro dessa pasta e de suas subpastas.

MAC (Media Access Control ou Message Authenticator Code)

Quanto ao primeiro, consulte Endereço MAC. O segundo é um código utilizado para identificar uma determinada mensagem (por exemplo, uma mensagem RADIUS). O código é geralmente uma mistura criptografada do conteúdo da mensagem, incluindo um valor exclusivo para proporcionar uma proteção contra reprodução.

mapa de rede

No Network Manager, uma representação gráfica dos computadores e componentes que fazem parte de uma rede doméstica.

navegador

Um programa cliente que usa o Hypertext Transfer Protocol (HTTP) para fazer solicitações de servidores Web na Internet. Um navegador da Web exibe o conteúdo de forma gráfica para o usuário.

Negação de serviço

Na Internet, um ataque de negação de serviço (DoS, denial of service) é um incidente no qual um usuário ou organização é privado dos serviços ou de um recurso que, em condições normais, estaria disponível. Tipicamente, a perda de serviços consiste na indisponibilidade de um determinado serviço de rede, como o e-mail, ou a perda temporária de todos os serviços e da conectividade de rede. Nos piores casos, por exemplo, um site acessado por milhões de pessoas pode, ocasionalmente, ser forçado a interromper temporariamente sua operação. Um ataque de negação de serviço também pode destruir a programação e os arquivos de um sistema de computador. Embora normalmente seja proposital e mal-intencionado, um ataque de negação de serviço pode, às vezes, ocorrer acidentalmente. Um ataque de negação de serviço é um tipo de violação de segurança em sistemas de computadores que não costuma resultar em roubo de informações ou em outras perdas de segurança. No entanto, esses ataques podem custar bastante tempo e dinheiro à pessoa ou empresa atingida.

NIC (Network Interface Card)

Uma placa que se conecta a um laptop ou a algum outro dispositivo e que conecta esse dispositivo à LAN.

palavra-chave

Um palavra que você pode atribuir a um arquivo com backup para estabelecer um relacionamento ou conexão com outros arquivos que possuam a mesma palavra-chave atribuída. Atribuir as palavras-chaves aos arquivos facilita a pesquisa pelos arquivos que você publicou na Internet.

phishing

Pronuncia-se "fishing", trata-se de uma fraude para roubar informações valiosas, como números de cartão de crédito e números de CPF, IDs de usuário e senha. Um e-mail aparentemente oficial é enviado a vítimas em potencial, fingindo ser de seus provedores de Internet, de bancos ou de lojas. Os e-mails podem ser enviados a pessoas em listas selecionadas ou em qualquer lista, esperando que alguma porcentagem dos destinatários tenha realmente uma conta na organização real.

placas adaptadoras sem fio PCI

Conecta um computador desktop a uma rede. A placa se conecta em um slot de expansão PCI dentro do computador.

placas adaptadoras sem fio USB

Oferece uma interface serial Plug and Play expansível. Essa interface proporciona uma conexão padrão sem fio e de baixo custo para dispositivos periféricos, como teclados, mouses, joysticks, impressoras, scanners, dispositivos de armazenamento e câmeras de videoconferência.

Ponto de acesso (PA)

Um dispositivo de rede que possibilita que clientes 802.11 se conectem a uma rede local (LAN). Os PAs estendem o alcance físico do serviço para usuários sem fio. Eles são ocasionalmente chamados de roteadores sem fio.

pontos de acesso ilícitos

Um ponto de acesso que uma empresa não autoriza para operação. O problema é que os pontos de acesso ilícitos normalmente não estão em conformidade com as políticas de segurança de LAN sem fio (WLAN). Um ponto de acesso ilícito permite uma interface aberta e desprotegida com a rede corporativa, partindo de fora do perímetro controlado fisicamente.

Dentro de uma WLAN devidamente protegida, pontos de acesso ilícitos são mais prejudiciais que usuários ilícitos. Usuários não autorizados tentando obter acesso a uma WLAN provavelmente não conseguirão atingir recursos corporativos valiosos se mecanismos de autenticação eficazes estiverem implementados. No entanto, problemas graves podem ocorrer quando um funcionário ou hacker se conecta a um ponto de acesso ilícito. Tal ponto de acesso permite que praticamente qualquer pessoa que tenha um dispositivo equipado com 802.11 entre na rede corporativa. Isso os coloca muito próximos a recursos de importância crucial.

pop-ups

Pequenas janelas que aparecem sobre outras janelas na tela de seu computador. As janelas pop-up geralmente são usadas nos navegadores da Web para exibir anúncios. A McAfee bloqueia as janelas pop-up que são carregadas automaticamente quando uma página da Web é carregada no navegador. As janelas pop-up que são carregadas quando você clica em um link não são bloqueadas pela McAfee.

porta

Local por onde as informações passam para entrar ou sair de um computador; por exemplo, um modem analógico convencional está conectado a uma porta serial. Os números de porta em comunicações TCP/IP são valores virtuais usados para separar tráfego em fluxos específicos de aplicativos. Portas são atribuídas a protocolos padrão como SMTP ou HTTP para que os programas saibam quais portas usar para tentar uma conexão. A porta de destino para pacotes TCP indica o aplicativo ou servidor procurado.

PPPoE

Point-to-Point Protocol Over Ethernet, um protocolo de comunicação. Usado por muitos provedores DSL, o PPPoE suporta a autenticação e as camadas de protocolo amplamente utilizadas no PPP, permitindo estabelecer uma conexão ponto a ponto na arquitetura habitualmente multiponto Ethernet.

programa potencialmente indesejado

Os programas potencialmente indesejados incluem spyware, adware e outros programas que coletam e transmitem seus dados sem a sua permissão.

protocolo

Um formato padronizado para transmissão de dados entre dois dispositivos. Do ponto de vista do usuário, o único aspecto interessante dos protocolos é que o computador ou dispositivo em questão precisa ter suporte para os protocolos apropriados, caso queira se comunicar com outros computadores. O protocolo pode ser implementado em hardware ou em software.

proxy

Um computador (ou software executado nele) que funciona como uma barreira entre uma rede e a Internet, apresentando somente um único endereço de rede para sites externos. Ao atuar como intermediário representando todos os computadores internos, o proxy protege identidades de rede ao mesmo tempo que oferece acesso à Internet. Consulte também servidor proxy.

publicar

Disponibilizar publicamente um arquivo com backup, na Internet.

quarentena

Quando arquivos suspeitos são detectados, eles ficam em quarentena. Em seguida, você pode executar a ação apropriada.

RADIUS (Remote Access Dial-In User Service)

Um protocolo que proporciona autenticação de usuários, normalmente numa situação de acesso remoto. Originalmente definido para uso com servidores de acesso remoto discado, o protocolo é atualmente usado em uma variedade de ambientes de autenticação, incluindo a autenticação 802.1x do segredo compartilhado do usuário de uma WLAN.

rede

Quando você conecta dois ou mais computadores, cria uma rede.

rede gerenciada

Uma rede doméstica gerenciada com dois tipos de membros: membros gerenciados e não gerenciados. Membros gerenciados permitem que outros computadores da rede monitores seu status de proteção McAfee, enquanto membros não gerenciados não o permitem.

repositório de backup on-line

O local no servidor on-line no qual seus arquivos de observação são armazenados depois de serem submetidos ao backup.

restaurar

Recuperar uma cópia de um arquivo a partir do arquivamento ou do repositório online de backup.

roaming

A capacidade de se passar da área de cobertura de um PA para a área de outro sem interrupção do serviço ou perda de conectividade.

roteador

Um dispositivo de rede que encaminha pacotes de uma rede para outra. Com base em tabelas de roteamento internas, os roteadores lêem cada pacote recebido e determinam como encaminhá-lo. A interface do roteador para a qual os pacotes transmitidos são enviados pode ser determinada por qualquer combinação de endereços de origem e de destino, bem como condições de tráfego atuais, como carga, custos das linhas ou linhas ruins. Os roteadores são, às vezes, chamados de pontos de acesso (PA).

script

Os scripts podem criar, copiar ou excluir arquivos. Eles também podem abrir o seu registro do Windows.

segredo compartilhado

Consulte também RADIUS. Protege partes sigilosas de mensagens RADIUS. Esse segredo compartilhado é uma senha compartilhada entre o autenticador e o servidor de autenticação de alguma maneira segura.

senha

Um código (geralmente alfanumérico) usado para obter acesso ao computador ou a um determinado programa ou site da Web.

servidor

Computador ou software que oferece serviços específicos a softwares em execução em outros computadores. O "servidor de email" de seu ISP é um software que lida com todas as mensagens enviadas e recebidas de todos os usuários. Um servidor em uma LAN é um hardware que constitui o principal nó da rede. Ele também pode conter softwares que oferecem serviços específicos, dados ou outros recursos a todos os computadores clientes a ele conectados.

servidor DNS

Abreviação para o servidor do Sistema de nomes de domínios. Um computador que pode responder a perguntas do Sistema de nomes de domínios (DNS). O servidor DNS mantém um banco de dados de computadores host e seus endereços IP correspondentes. A receber o nome apex.com, por exemplo, o servidor DNS retornaria o endereço IP da empresa hipotética Apex. Também denominado: servidor de nomes. Consulte também DNS e endereço IP.

Servidor proxy

Um componente de firewall que gerencia o tráfego da Internet de e para uma rede local (LAN). Um servidor proxy pode melhorar o desempenho ao oferecer dados solicitados com freqüência, como uma página popular da Web, e pode filtrar e descartar solicitações que o proprietário não considera apropriadas, como solicitações de acesso não autorizado a arquivos patenteados.

servidor SMTP

Acrônimo para Simple Mail Transfer Protocol (protocolo de transferência de correio simples). Um protocolo TCP/IP para enviar mensagens de um computador a outro em uma rede. Esse protocolo é usado na Internet para rotear o e-mail.

sincronizar

Resolver as inconsistências entre os arquivos do backup e os armazenados em seu computador local. Os arquivos são sincronizados quando a versão do arquivo no repositório on-line de backup for mais recente que a versão do arquivo em outros computadores. A sincronização atualiza a cópia do arquivo em seus computadores com a versão do arquivo no repositório de backup on-line.

sobrecarga de buffer

Sobrecargas de buffer ocorrem quando programas ou processos suspeitos tentam armazenar dados em um buffer (área de armazenagem temporária de dados) além de seu limite, corrompendo ou sobrescrevendo dados válidos em buffers adjacentes.

SSID (Service Set Identifier)

Nome de rede para os dispositivos de um subsistema de LAN sem fio. Trata-se de uma seqüência de 32 caracteres de texto simples acrescentada ao cabeçalho de todo pacote WLAN. O SSID diferencia uma WLAN de outra, portanto, todos os usuários de uma rede precisam fornecer o mesmo SSID para ter acesso a um determinado PA. Um SSID impede o acesso de qualquer dispositivo cliente que não tenha o SSID. Contudo, o ponto de acesso (PA) divulga, por padrão, seu SSID ao se anunciar. Mesmo que a divulgação de SSID esteja desativada, um hacker pode detectar o SSID através de farejamento (sniffing).

SSL (Secure Sockets Layer)

Um protocolo desenvolvido pela Netscape para transmissão de documentos privados pela Internet. A SSL funciona utilizando uma chave pública para criptografar dados que é transferida através da conexão SSL. Tanto o Netscape Navigator quanto o Internet Explorer usam e suportam SSL, e muitos sites usam esse protocolo para obter informações confidenciais do usuário, como números de cartão de crédito. Por uma questão de convenção, os URLs que exigem uma conexão SSL começam com https: em vez de http:

SystemGuard

Os SystemGuards detectam alterações não autorizadas em seu computador e alertam você quando elas ocorrem.

texto codificado

Dados que foram criptografados. O texto codificado é ilegível até ser convertido em texto simples (descriptografado) com uma chave.

texto simples

Qualquer mensagem que não esteja criptografada.

tipos de arquivos observados

Os tipos de arquivos (por exemplo, .doc, .xls e assim por diante) que o Data Backup submete a backup ou arquiva dentro dos locais de observação.

TKIP (Temporal Key Integrity Protocol)

Uma correção rápida para superar as vulnerabilidades inerentes à segurança WEP, especialmente a reutilização de chaves de criptografia. O TKIP altera as chaves temporais a cada 10.000 pacotes, proporcionando um método de distribuição dinâmico que melhora significativamente a segurança da rede. O processo (de segurança) TKIP começa com uma chave temporal de 128 bits compartilhada entre clientes e pontos de acesso (PAs). O TKIP combina a chave temporal com o endereço MAC (da máquina cliente) e, em seguida, adiciona um vetor de inicialização relativamente grande de 16 octetos para produzir a chave que criptografa os dados. Esse procedimento garante que cada estação utilize fluxos de chaves diferentes para criptografar os dados. O TKIP usa RC4 para realizar a criptografia. A WEP também usa RC4.

unidade de rede

Uma unidade de disco ou de fita que é conectada a um servidor em uma rede compartilhada por vários usuários. Às vezes, as unidades de rede são denominadas unidades remotas.

URL

Uniform Resource Locator (URL - Localizador Uniforme de Recursos). É o formato padrão para endereços da Internet.

varredura em tempo real

É feita a varredura nos arquivos em busca de vírus e outras atividades quando eles forem acessados por você ou por seu computador.

VPN (Virtual Private Network (Rede virtual privada))

Uma rede construída pela utilização de cabeamento público para reunificar nós. Existem, por exemplo, vários sistemas que permitem criar redes utilizando a Internet como meio para transporte de dados. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede e que os dados não possam ser interceptados.

wardriver

Pessoas munidas de laptops, software especial e algum hardware alternativo que circulam de carro por cidades, bairros e estacionamentos de empresas com o objetivo de interceptar tráfego de LAN sem fio.

Web bugs

Arquivos gráficos pequenos que podem ser incorporados em suas páginas HTML e que permitem que uma origem não autorizada configure os cookies em seu computador. Esses cookies podem então transmitir as informações para a origem não autorizada. Os Web bugs também são denominados beacons da Web, marcas de pixel, GIFs de limpeza ou GIFs invisíveis.

WEP (Wired Equivalent Privacy)

Um protocolo de criptografia e autenticação definido como parte do padrão 802.11. Suas versões iniciais baseiam-se em codificadores RC4 e possuem vulnerabilidades significativas. A WEP tenta proporcionar segurança criptografando os dados através de ondas de rádio, para que eles estejam protegidos ao serem transmitidos de um ponto para outro. No entanto, descobriu-se que a WEP não é tão segura quanto se acreditava.

Wi-Fi (Wireless Fidelity)

Termo utilizado genericamente em referência a qualquer tipo de rede 802.11, seja 802.11b, 802.11a, banda dupla, etc. O termo é empregado pela Wi-Fi Alliance.

Wi-Fi Alliance

Uma organização composta pelos maiores fornecedores de software e equipamentos de comunicação sem fio com o objetivo de (1) certificar todos os produtos com base no 802.11 quanto a interoperabilidade e (2) promover o termo Wi-Fi como marca global em todos os mercados para qualquer produto de LAN sem fio com base no 802.11. A organização atua como associação, laboratório de testes e agência reguladora para fornecedores que queiram promover a interoperabilidade e o crescimento da indústria.

Embora todos os produtos 802.11a/b/g sejam chamados Wi-Fi, somente produtos que tenham passado pelos testes da Wi-Fi Alliance podem ser denominados Wi-Fi Certified (uma marca registrada). Os produtos que são aprovados devem levar um selo de identificação em suas embalagens dizendo Wi-Fi Certified e que indique a banda de freqüências de rádio utilizada. Esse grupo era conhecido como Wireless Ethernet Compatibility Alliance (WECA), mas mudou de nome em outubro de 2002 para refletir melhor a marca Wi-Fi que desejava construir.

Wi-Fi Certified

Quaisquer produtos testados e aprovados como Wi-Fi Certified (uma marca registrada) pela Wi-Fi Alliance são certificados quanto a interoperabilidade mútua, mesmo que sejam de fabricantes diferentes. Um usuário com um produto Wi-Fi Certified pode usar qualquer marca de ponto de acesso (PA) com qualquer outra marca de hardware cliente que também seja certificado. Geralmente, porém, qualquer produto Wi-Fi que utilize a mesma freqüência de rádio (por exemplo, 2,4 GHz para 802.11b ou 11g e 5 GHz para 802.11a) funciona com outro, mesmo que não seja Wi-Fi Certified.

WLAN (Wireless Local Area Network)

Consulte também LAN. Uma rede local que utiliza um meio sem fio para conexão. Uma WLAN usa ondas de rádio de alta freqüência em vez de fios para comunicação entre os nós.

worm

Um worm é um vírus que se replica automaticamente na memória ativa e que pode enviar cópias de si mesmo através de mensagens de e-mail. Os worms replicam e consomem recursos do sistema, reduzindo o desempenho ou interrompendo as tarefas.

WPA (Wi-Fi Protected Access)

Um padrão de especificação que aumenta muito o nível de proteção de dados e controle de acesso para sistemas de LAN sem fio futuros e existentes. Desenvolvido para ser executado em hardware existente ou como uma atualização de software, o WPA é derivado do padrão IEEE 802.11i, sendo compatível com este. Quando instalado corretamente, proporciona aos usuários de LAN sem fio um elevado grau de garantia de que seus dados permaneçam protegidos e que apenas usuários de rede autorizados tenham acesso à rede.

WPA-PSK

Um modo especial de WPA desenvolvido para usuários domiciliares que não precisam de uma segurança tão forte quanto a de empresas e que não têm acesso a servidores de autenticação. Nesse modo, o usuário domiciliar digita manualmente a senha inicial para ativar o Wi-Fi Protected Access (WPA) em modo pré-compartilhado (Pre-Shared Key ou PSK), devendo ele próprio alterar a frase de senha de cada computador e ponto de acesso sem fio regularmente. Consulte também WPA2-PSK e TKIP.

WPA2

Consulte também WPA. WPA2 é uma atualização do padrão de segurança WPA e é baseada no padrão 802.11i IEEE.

WPA2-PSK

Consulte também WPA-PSK e WPA2. WPA2-PSK é semelhante ao WPA-PSK e é baseado no padrão WPA2. Um recurso comum do WPA2-PSK é que os dispositivos geralmente suportam vários modos de criptografia (por exemplo, AES, TKIP) simultaneamente, enquanto os dispositivos mais antigos geralmente suportavam apenas em um único modo de criptografia por vez (ou seja, todos os clientes teriam que usar o mesmo modo de criptografia).

Sobre a McAfee

A McAfee, Inc., com sede em Santa Clara, Califórnia, e líder mundial em prevenção de invasões e gerenciamento de riscos à segurança, fornece soluções e serviços proativos comprovados que protegem sistemas e redes em todo o mundo. Com sua experiência inigualável em segurança e compromisso com a inovação, a McAfee confere a usuários domésticos, empresas públicas e privadas, e provedores de serviços a capacidade de bloquear ataques, evitar problemas e rastrear e aprimorar continuamente sua segurança.

Copyright

Índice

B

C

Ch

C

M

N

O

P

Q

R